Bearbeitungsstand: 14.07.2020 16:41 Uhr

Referentenentwurf

des Bundesministeriums für Wirtschaft und Energie

Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze

A. Problem und Ziel

Die Datenschutz-Grundverordnung (DSGVO) (Verordnung (EU) 2016/679) gilt seit dem 25. Mai 2018 auch für den Schutz der personenbezogenen Daten im Bereich der Telemedien und der Telekommunikation. Datenschutzbestimmungen des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) werden durch die Bestimmungen der DSGVO verdrängt, soweit nicht Öffnungsklauseln der DSGVO den Mitgliedstaaten die Möglichkeit geben, eigene Regelungen zu treffen. Weiterhin bleibt die Richtlinie 2002/58/EG, in der durch die Richtlinie 2009/136/EG geänderten Fassung(E-Privacy-Richtlinie), aufrechterhalten. Bestimmungen des TKG, die diese umsetzen, gelten weiterhin. Das Nebeneinander von DSGVO, TMG und TKG führt zu Rechtsunsicherheiten bei Verbrauchern, die Telemedien und elektronischen Kommunikationsdienste nutzen, bei Anbietern von diesen Diensten und bei den Aufsichtsbehörden. Der vorliegende Gesetzentwurf soll für Rechtsklarheit sorgen. Die Neuregelung soll auch dazu dienen, die Verwirklichung eines wirksamen und handhabungsfreundlichen Datenschutzes und Schutzes der Privatsphäre zu erleichtern, insbesondere mit Blick auf die in vielen Fällen erforderliche Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten oder in das Speichern und Abrufen von Informationen auf Endeinrichtungen der Endnutzer. Hier soll eine Rechtsgrundlage für die rechtssichere und wirksame Einbindung von anerkannten Diensten zur Verwaltung persönlicher Informationen (Personal Information Management Services) geschaffen werden. Der Gesetzentwurf zielt darauf ab, einen wirksamen Datenschutz und Schutz der Privatsphäre der Endnutzer zu gewährleisten. Dabei sollen aber funktionierende Geschäftsmodelle weder beeinträchtigt noch Innovationen in der digitalen Welt behindert werden, insbesondere mit Blick auf das Internet der Dinge und die Marktposition kleiner und mittlere Unternehmen sowie Start-ups im Online-Handel gegenüber den großen den Markt dominierenden Unternehmen. Die Aufsicht im Bereich des Telekommunikationsdatenschutzes soll, was den Schutz der personenbezogenen Daten natürlicher Personen anbelangt, zukünftig auf den oder die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit übergehen.

B. Lösung

Die Datenschutz-Bestimmungen des TMG und des TKG, einschließlich der Bestimmungen zum Schutz des Fernmeldegeheimnisses, sollen aufgehoben und in einem neuen Gesetz zusammengeführt werden. Dabei sollen zugleich die erforderlichen Anpassungen an die DSGVO erfolgen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

Es entsteht kein über die bereits bestehenden Regelungen der DSGVO und zur Umsetzung der E-Privacy-Richtlinie hinausgehender Erfüllungsaufwand für die Wirtschaft.

Davon Bürokratiekosten aus Informationspflichten

Entbehrlich (s.o.).

E.3 Erfüllungsaufwand der Verwaltung

Es entsteht Erfüllungsaufwand beim Bund dadurch, dass zukünftig bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zusätzliche Aufgaben im Bereich der Aufsicht im Bereich der elektronischen Kommunikationsdienste erwachsen, zum einen dadurch, dass zukünftig auch nummernunabhängige interpersonelle Kommunikationsdienste zu beaufsichtigen sind, und zum anderen dadurch, dass bei der Aufsicht über die Bestimmungen zum Schutz der personenbezogenen Daten eine umfassende Tätigkeit der oder des BfDI als unabhängiger Datenschutzaufsichtsbehörde zu gewährleisten ist.

F. Weitere Kosten

Weitere Kosten für die Wirtschaft, Kosten für soziale Sicherungssysteme, Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

Referentenentwurf des Bundesministeriums für Wirtschaft und Energie

Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien[1)]

(Telekommunikations-Telemedien-Datenschutz-Gesetz – TTDSG)

Teil 1

Allgemeine Vorschriften

§ 1

Geltungsbereich

(1) Dieses Gesetz regelt den Schutz personenbezogener Daten der Endnutzer von elektronischer Kommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig elektronische Kommunikationsdienste in öffentlichen elektronischen Kommunikationsnetzen, einschließlich öffentlicher elektronischer Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken, und von Telemedien. Die Bestimmungen der Verordnung (EU) 2016/679 bleiben im Übrigen unberührt

(2) 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.

[1)] 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 wurde.

§ 2

Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. ist „elektronische Kommunikation“ der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen;

2. ist „öffentliches elektronisches Kommunikationsnetz“ ein Kommunikationsnetz, das ganz oder überwiegend der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen;

3. ist "Diensteanbieter" jeder, der ganz oder teilweise geschäftsmäßig elektronische Kommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt;

4. sind "Bestandsdaten" Daten eines Endnutzers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über elektronische Kommunikationsdienste erhoben werden;

5. sind „Verkehrsdaten“ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

6. sind „Standortdaten“ Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

7. ist „Nachricht“ jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst ausgetauscht oder weitergeleitet wird;

8. sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;

9. ist „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

10. ist „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten; dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

11. ist „Dienst mit Zusatznutzen“ jeder Dienst, der die Bearbeitung von Verkehrsdaten oder anderer Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

12. ist „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;

13. sind „elektronische Kommunikationsdienste“ Internetzugangsdienste, interpersonelle Kommunikationsdienste und Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, soweit sie in der Regel gegen Entgelt über elektronische Kommunikationsnetze erbracht werden;

14. ist „Internetzugangsdienst“ jeder öffentlich zugängliche elektronische Kommunikationsdienst, der unabhängig von der verwendeten Netztechnologie und den verwendeten Endgeräten Zugang zum Internet und somit Verbindungen zu praktisch allen Abschlusspunkten des Internets bietet;

15. ist „interpersoneller Kommunikationsdienst“ ein gewöhnlich gegen Entgelt erbrachter Dienst, der die Übermittlung von Informationen über elektronische Kommunikationsnetze an vom Absender bestimmte Personen ermöglicht; dazu zählen keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen;

16. ist „Nutzer“ eine natürliche oder juristische Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst in Anspruch nimmt oder beantragt;

17. ist „Endnutzer“ ein Nutzer, der keine öffentlichen elektronischen Kommunikationsnetze oder öffentlich zugänglichen elektronischen Kommunikationsdienste bereitstellt;

18. sind „Endeinrichtungen“ direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtungen zum Aussenden, Verarbeiten oder Empfangen von Nachrichten;

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

§ 3

Anerkannte Dienste zur Verwaltung persönlicher Informationen

(1) Endnutzer können ihre Rechte nach diesem Gesetz über anerkannte Dienste, die die Verwaltung persönlicher Informationen anbieten, ausüben. Dazu zählt insbesondere die Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten sowie in das Speichern von Informationen auf ihren Endeinrichtungen und den Zugriff auf Informationen, die bereits auf ihren Endeinrichtungen gespeichert sind. Vereinbarungen zwischen Endnutzern und Diensteanbietern nach Satz 1 sind nur wirksam, wenn die Endnutzer freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich erklären oder sonst eindeutig bestätigen, dass sie mit der Ausübung ihrer Rechte durch den Dienst einverstanden sind. Die Freiwilligkeit ist nicht gegeben, wenn Endnutzer nur mit bestimmten Diensten Vereinbarungen zur Verwaltung persönlicher Informationen treffen dürfen oder die Erbringung eines Telemedien- oder elektronischen Kommunikationsdienstes von der Inanspruchnahme von Diensten zur Verwaltung persönlicher Informationen abhängig gemacht wird.

(2) Dienste, die die Verwaltung persönlicher Informationen anbieten, können unter der Voraussetzung anerkannt werden, dass sie kein wirtschaftliches Eigeninteresse an den im Auftrag der Endnutzer verwalteten Daten haben und zudem unabhängig von Unternehmen sind, die ein solches Interesse haben können. Die Anerkennung setzt weiter-

hin voraus, dass die Dienste ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes ermöglicht. Dies gilt insbesondere im Hinblick auf den Nachweis, dass der Dienst sowohl technisch als auch organisatorisch in der Lage ist, die Anforderungen an den Datenschutz und die Datensicherheit, die sich aus der Verordnung (EU) 2016/679 ergeben, zu erfüllen.

(3) Zuständig für die Anerkennung von Diensten zur Verwaltung persönlicher Informationen ist der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Teil 2

Datenschutz und Schutz der Privatsphäre in der elektronischen Kommunikation

§ 4

Vertraulichkeit der Kommunikation – Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der elektronischen Kommunikation 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) Anbieter elektronischer Kommunikationsdienste und -netze sind zur Wahrung des Fernmeldegeheimnisses verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der elektronischen Kommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der elektronischen Kommunikation 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 elektronische Kommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

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

§ 5

Verlangen eines amtlichen Ausweises

Der Diensteanbieter kann im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von öffentlich zugänglichen elektronischen Kommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Endnutzers erforderlich ist. Der Endnutzer kann dazu den elektronischen Identitätsnachweis gemäß § 18 Personalausweisgesetz nutzen.

Die Pflicht nach § 111 Absatz 1 Satz 3 des Telekommunikationsgesetzes bleibt unberührt. Er kann von dem Ausweis eine Kopie erstellen. Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Endnutzers zu vernichten.

§ 6

Abhörverbot, Geheimhaltungspflicht der Betreiber von Funkanlagen

Mit einer Funkanlage (§ 1 Nummer 1 Funkanlagengesetz) dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateure im Sinne des Gesetzes über den Amateurfunk vom 23. Juni 1997 (BGBl. I S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört oder in vergleichbarer Weise zur Kenntnis genommen werden. Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 3 besteht, anderen nicht mitgeteilt werden. § 3 Absatz 4 gilt entsprechend. Das Abhören oder die in vergleichbarer Weise erfolgende Kenntnisnahme und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.

§ 7

Missbrauch von Telekommunikationsanlagen

(1) Es ist verboten, Telekommunikationsanlagen zu besitzen, herzustellen oder auf dem Markt bereitzustellen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen. Als zum unbemerkten Abhören oder Aufnehmen eines Bildes bestimmt gilt eine Telekommunikationsanlage insbesondere, wenn diese Aufnahmefunktion beim bestimmungsgemäßen Gebrauch des Gegenstandes für den Betroffenen nicht eindeutig erkennbar ist. Das Verbot, solche Anlagen zu besitzen, gilt nicht für denjenigen, der die tatsächliche Gewalt über eine solche Anlage

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

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

3. als Gerichtsvollzieher oder Vollzugsbeamter in einem Vollstreckungsverfahren erwirbt,

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

5. lediglich zur gewerbsmäßigen Beförderung oder gewerbsmäßigen Lagerung erlangt,

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

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

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

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

(3) 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 dessen Bild von diesem unbemerkt aufzunehmen.

(4) Zur Verfolgung von Verstößen gegen die Verbote des Absatzes 1 kann die Bundesnetzagentur von Verkäufern und Betreibern von Verkaufsplattformen Auskünfte zu personenbezogenen Daten von Käufern und Verkäufern verbotener Telekommunikationsanlagen wie Name und Anschrift sowie Kauf- und Versanddatum verlangen, soweit sie für den Vollzug dieses Gesetzes erforderlich sind. Verkäufer und Plattformbetreiber dürfen auf Anordnung der Bundesnetzagentur die nach Satz 1 abgefragten personenbezogenen Daten an die Bundesnetzagentur übermitteln.

§ 8

Nachrichtenübermittlung mit Zwischenspeicherung

(1) Anbieter elektronischer Kommunikationsdienste dürfen bei Diensten, für deren Durchführung eine Zwischenspeicherung erforderlich ist, Nachrichteninhalte, insbesondere Sprach-, Ton-, Text- und Grafikmitteilungen von Teilnehmern, im Rahmen eines hierauf gerichteten Diensteangebots unter folgenden Voraussetzungen verarbeiten:

1. Die Verarbeitung erfolgt ausschließlich in Telekommunikationsanlagen des zwischenspeichernden Diensteanbieters, es sei denn, die Nachrichteninhalte werden im Auftrag des Endnutzers oder durch Eingabe des Endnutzers in Telekommunikationsanlagen anderer Diensteanbieter weitergeleitet.

2. Ausschließlich der Endnutzer bestimmt durch seine Eingabe Inhalt, Umfang und Art der Verarbeitung.

3. Ausschließlich der Endnutzer bestimmt, wer Nachrichteninhalte eingeben und darauf zugreifen darf (Zugriffsberechtigter).

4. Der Diensteanbieter darf dem Endnutzer mitteilen, dass der Empfänger auf die Nachricht zugegriffen hat.

5. Der Diensteanbieter darf Nachrichteninhalte nur entsprechend dem mit dem Endnutzer geschlossenen Vertrag löschen.

(2) Der Diensteanbieter hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nach-

richteninhalten 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.

§ 9

Einwilligung bei Endeinrichtungen

(1) Das Speichern von Informationen auf Endeinrichtungen des Endnutzers oder der Zugriff auf Informationen, die bereits in seinen Endeinrichtungen des Endnutzers gespeichert sind, ist nur erlaubt, wenn der Endnutzer darüber gemäß der Verordnung (EU) 2016/679 informiert wurde und er eingewilligt hat.

(2) Absatz 1 gilt nicht, wenn die Speicherung von Informationen auf Endeinrichtungen oder der Zugriff auf Informationen, die bereits in Endeinrichtungen gespeichert sind,

1. technisch erforderlich ist, um eine Kommunikation über ein elektronisches Kommunikationsnetz zu übermitteln oder um Telemedien bereitzustellen, deren Inanspruchnahme vom Endnutzer gewünscht wird,

2. vertraglich ausdrücklich mit dem Endnutzer vereinbart wurde, um bestimmte Dienstleistungen zu erbringen, oder

3. zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist.

(3) Im Falle der Inanspruchnahme von Telemedien liegt eine wirksame Einwilligung in die Speicherung von Informationen auf Endeinrichtungen oder in den Zugriff auf Informationen, die bereits in Endeinrichtungen gespeichert sind, vor,

1. wenn der Diensteanbieter den Endnutzer darüber informiert hat, welche Informationen zu welchem Zweck und wie lange auf Endeinrichtungen gespeichert bleiben und ob Dritte Zugriff auf diese Informationen erhalten, und

2. der Endnutzer mittels einer Funktion diese Information aktiv bestätigt und die Telemedien in Anspruch nimmt.

(4) Der Endnutzer kann die Einwilligung auch erklären, in dem er eine dafür vorgesehene Einstellung seines Browsers oder eine andere Anwendung auswählt.

§ 10

Verkehrsdaten

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

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

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

3. den vom Nutzer in Anspruch genommenen elektronischen Kommunikationsdienst,

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 elektronischen Kommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

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

(2) Eine über Absatz 1 hinausgehende Verarbeitung der Verkehrsdaten ist unzulässig.

(3) Der Diensteanbieter darf Verkehrsdaten zum Zwecke der Vermarktung von elektronischen Kommunikationsdiensten, zur bedarfsgerechten Gestaltung von elektronischen Kommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und im dazu erforderlichen Zeitraum nur verarbeiten, wenn der Endnutzer eingewilligt hat. Die Daten der Angerufenen sind unverzüglich zu anonymisieren. Eine zielnummernbezogene Verwendung der Verkehrsdaten durch den Diensteanbieter zu den in Satz 1 genannten Zwecken ist nur mit Einwilligung der Angerufenen zulässig. Hierbei sind die Daten der Anrufenden unverzüglich zu anonymisieren.

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

§ 11

Entgeltermittlung und Entgeltabrechnung

(1) Diensteanbieter dürfen die in § 10 Absatz 1 aufgeführten Verkehrsdaten nach Maßgabe der Absätze 2 bis 4 verarbeiten, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Endnutzern benötigt werden. Erbringt ein Diensteanbieter seine Dienste über ein öffentliches elektronisches Kommunikationsnetz eines fremden Betreibers, darf der Betreiber des öffentlichen Telekommunikationsnetzes dem Diensteanbieter die für die Erbringung von dessen Diensten erhobenen Verkehrsdaten übermitteln. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er dem Dritten die in Absatz 2 genannten Daten übermitteln, soweit es zum Einzug des Entgelts und der Erstellung einer detaillierten Rechnung erforderlich ist. Der Dritte ist vertraglich zur Wahrung des Fernmeldegeheimnisses und des Datenschutzes zu verpflichten. Die Bestimmungen der Verordnung (EU) 2016/679 bleiben unberührt.

(2) Der Diensteanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 10 Absatz 1 Nummern 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 Diensteanbieters mit anderen Diensteanbietern oder mit deren Endnutzern sowie anderer Diensteanbieter mit ihren Endnutzern erforderlich ist, darf der Diensteanbieter Verkehrsdaten verarbeiten.

(4) Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von elektronischen Kommunikationsdiensten erbracht hat, so darf er dem Dritten Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Endnutzer erforderlich sind.

§ 12

Einzelverbindungsnachweis

(1) Dem Endnutzer sind die gespeicherten Daten derjenigen Anrufe, für die er entgeltpflichtig ist, nur dann mitzuteilen, wenn er vor dem maßgeblichen Abrechnungszeitraum in Textform einen Einzelverbindungsnachweis verlangt hat. Auf Wunsch dürfen ihm auch die Daten pauschal abgegoltener Verbindungen mitgeteilt werden. Dabei entscheidet der Endnutzer, ob ihm die von ihm gewählten Rufnummern ungekürzt oder unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Bei Mehrpersonenhaushalten mit nur einem Teilnehmeranschluss ist die Mitteilung nur zulässig, wenn der Endnutzer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitnutzer seines Teilnehmeranschlusses darüber informiert hat und künftige Mitnutzer unverzüglich darüber informieren wird, dass dem Anschlussinhaber die Rufnummern zur Erteilung des Verbindungsnachweises bekannt gegeben werden. Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Endnutzer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. Soweit die öffentlich-rechtlichen Religionsgesellschaften für ihren Bereich eigene Mitarbeitervertreterregelungen erlassen haben, findet Satz 4 mit der Maßgabe Anwendung, dass an die Stelle des Betriebsrates oder der Personalvertretung die jeweilige Mitarbeitervertretung tritt. Dem Endnutzer dürfen darüber hinaus die gespeicherten Daten mitgeteilt werden, wenn er Einwendungen gegen die Höhe der Verbindungsentgelte erhoben hat. 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 ausgehen, nur unter Kürzung um die letzten drei Ziffern mitgeteilt werden. Die Sätze 2 und 7 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

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

Die Sätze 1 bis 6 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.

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

§ 13

Störungen von Telekommunikationsanlagen und Missbrauch von elektronischen Kommunikationsdiensten

(1) Soweit erforderlich, darf der Diensteanbieter die Verkehrsdaten der Endnutzer verarbeiten, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Das gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Eine Nutzung der Daten zu anderen Zwecken ist unzulässig. Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der betriebliche Datenschutzbeauftragte unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden.

(2) Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der betriebliche Datenschutzbeauftragte unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. Im Übrigen muss der Diensteanbieter dem betrieblichen Datenschutzbeauftragten und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen in diesem Zeitraum schriftlich berichten. Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit leitet diese Informationen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Der Betroffene ist von dem Diensteanbieter zu benachrichtigen, sofern dieser ermittelt werden kann. Wurden im Rahmen einer Maßnahme nach Satz 1 auch Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung verarbeitet, müssen die Berichte mindestens auch Angaben zum Umfang und zur Erforderlichkeit der Erhebung und Verwendung der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung enthalten.

(3) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. Eventuelle bei der Aufschaltung erstellte Aufzeichnungen sind unverzüglich zu löschen. Das Aufschalten muss den betroffenen Kommunikationsteilnehmern durch ein akustisches oder sonstiges Signal zeitgleich angezeigt und ausdrücklich mitgeteilt werden. Sofern dies technisch nicht möglich ist, muss der betriebliche Datenschutzbeauftragte unverzüglich detailliert über die Verfahren und Umstände jeder einzelnen Maßnahme informiert werden. Diese Informationen sind beim betrieblichen Datenschutzbeauftragten für zwei Jahre aufzubewahren.

(4) Wenn zu dokumentierende tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Telekommunikationsnetzes oder -dienstes vorliegen, insbesondere für eine Leistungserschleichung oder einen Betrug oder eine unzumutbare Belästigung nach § 7 des Gesetzes gegen den unlauteren Wettbewerb, darf der Diensteanbieter zur Sicherung seines Entgeltanspruchs sowie zum Schutz der Endnutzer vor rechtswidriger Kommunikation Verkehrsdaten verarbeiten, die erforderlich sind, um die rechtswidrige

Inanspruchnahme des Telekommunikationsnetzes oder -dienstes aufzudecken und zu unterbinden. Der Diensteanbieter darf die Verkehrsdaten in der Weise verarbeiten, dass aus dem Gesamtbestand aller Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen. Der Diensteanbieter darf aus den Verkehrsdaten nach Satz 1 einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von einzelnen Teilnehmern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Kriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer rechtswidrigen Inanspruchnahme besteht. Die Daten anderer Verbindungen sind unverzüglich zu löschen. Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.

§ 14

Standortdaten

(1) Sofern der Dienstenanbieter Standortdaten von Endnutzern verarbeitet, die nicht Verkehrsdaten sind, dürfen diese ohne Einwilligung des Endnutzers nur verarbeitet werden, soweit und solange dies zur Bereitstellung von Diensten mit Zusatznutzen erforderlich ist, wenn sie anonymisiert wurden. In diesen Fällen hat der Anbieter des Dienstes mit Zusatznutzen bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Endnutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, zu informieren. Dies gilt nicht, wenn der Standort nur auf dem Endgerät angezeigt wird, dessen Standortdaten ermittelt wurden. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Inhaber des Teilnehmeranschlusses oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Inhaber des Teilnehmeranschlusses seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen. In diesem Fall gilt die Verpflichtung nach Satz 2 entsprechend für den Anbieter des Dienstes mit Zusatznutzen. Der Anbieter des Dienstes mit Zusatznutzen darf die erforderlichen Bestandsdaten zur Erfüllung seiner Verpflichtung aus Satz 2 nutzen. Der Inhaber des Teilnehmeranschlusses muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden.

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

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

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

§ 15

Mitteilen ankommender Verbindungen

(1) Trägt ein Endnutzer in einem zu dokumentierenden Verfahren schlüssig vor, dass bei seinem Anschluss bedrohende oder belästigende Anrufe ankommen, hat der Diensteanbieter auf schriftlichen Antrag auch netzübergreifend Auskunft über die Inhaber der Anschlüsse zu erteilen, von denen die Anrufe ausgehen. Die Auskunft darf sich nur auf Anrufe beziehen, die nach Stellung des Antrags durchgeführt werden. Der Diensteanbieter darf die Rufnummern, Namen und Anschriften der Inhaber dieser Anschlüsse sowie Datum und Uhrzeit des Beginns der Verbindungen und der Verbindungsversuche verarbeiten sowie diese Daten seinem Endnutzer mitteilen. Die Sätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur geschlossenen Benutzergruppen anbieten.

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

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

(4) Der Inhaber des Anschlusses, von dem die festgestellten Verbindungen ausgegangen sind, ist zu unterrichten, dass über diese Auskunft erteilt wurde. Davon kann abgesehen werden, wenn der Antragsteller schriftlich schlüssig vorgetragen hat, dass ihm aus dieser Mitteilung wesentliche Nachteile entstehen können, und diese Nachteile bei Abwägung mit den schutzwürdigen Interessen der Anrufenden als wesentlich schwerwiegender erscheinen. Erhält der Endnutzer, 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) Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist über die Einführung und Änderung des Verfahrens zur Sicherstellung der Absätze 1 bis 4 unverzüglich in Kenntnis zu setzen.

§ 16

Rufnummernanzeige und -unterdrückung

(1) Bietet der Diensteanbieter die Anzeige der Rufnummer der Anrufenden an, so müssen Anrufende und Angerufene die Möglichkeit haben, die Rufnummernanzeige dauernd oder für jeden Anruf einzeln auf einfache Weise und unentgeltlich zu unterdrücken. Angerufene müssen die Möglichkeit haben, eingehende Anrufe, bei denen die Rufnummernanzeige durch den Anrufenden unterdrückt wurde, auf einfache Weise und unentgeltlich abzuweisen. Wird die Anzeige der Rufnummer von Angerufenen angeboten, so müssen Angerufene die Möglichkeit haben, die Anzeige ihrer Rufnummer beim Anrufenden auf einfache Weise und unentgeltlich zu unterdrücken. Dies gilt auch für Anrufe in das Ausland und für aus dem Ausland kommende Anrufe, soweit sie Anrufende oder Angerufene im Inland betreffen. Bei Verbindungen zu Anschlüssen, die unter den Notrufnummern 112 oder 110 oder der Rufnummer 124 124 oder 116 117 erreicht werden, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Anzeige von Nummern der Anrufenden ausgeschlossen wird

(2) Abweichend von Absatz 1 Satz 1 dürfen Anrufende bei Werbung mit einem Telefonanruf ihre Rufnummernanzeige nicht unterdrücken oder bei dem Diensteanbieter veranlassen, dass diese unterdrückt wird; der Anrufer hat sicherzustellen, dass dem Angerufenen die dem Anrufer zugeteilte Rufnummer übermittelt wird.

(3) Die Absätze 1 und 2 gelten nicht für Diensteanbieter, die ihre Dienste nur den Teilnehmern geschlossener Benutzergruppen anbieten.

(4) Auf Antrag des Teilnehmers muss der Diensteanbieter Anschlüsse bereitstellen, bei denen die Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, an den angerufenen Anschluss unentgeltlich ausgeschlossen ist. Die Anschlüsse sind auf Antrag des Teilnehmers im Endnutzerverzeichnis (§ 18) seines Diensteanbieters zu kennzeichnen. Ist eine Kennzeichnung nach Satz 2 erfolgt, so darf an den so gekennzeichneten Anschluss eine Übermittlung der Rufnummer des Anschlusses, von dem der Anruf ausgeht, erst dann erfolgen, wenn zuvor die Kennzeichnung in der aktualisierten Fassung des Teilnehmerverzeichnisses nicht mehr enthalten ist.

(5) Hat der Teilnehmer die Eintragung in das Teilnehmerverzeichnis nicht nach § 18 beantragt, unterbleibt die Anzeige seiner Rufnummer bei dem angerufenen Anschluss, es sei denn, dass der Teilnehmer die Übermittlung seiner Rufnummer ausdrücklich wünscht.

§ 17

Automatische Anrufweiterschaltung

Der Diensteanbieter ist verpflichtet, seinen Endnutzern 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 Endnutzern anbieten.

§ 18

Endnutzerverzeichnisse

(1) Endnutzer können mit ihrer Rufnummer, ihrem Namen, ihrer Anschrift und zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses gedruckte oder elektronische Verzeichnisse die der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglich sind, eingetragen werden, soweit sie dies beantragen. Dabei können die Teilnehmer bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen. Auf Verlangen des Endnutzers dürfen Mitbenutzer des Anschlusses eingetragen werden, soweit diese damit einverstanden sind.

(2) Der Anbieter eines rufnummernabhängigen elektronischen Kommunikationsdienstes hat den Endnutzer unentgeltlich über die Möglichkeit der Aufnahme seiner Rufnummer, seines Namens, seines Vornamens seiner Anschrift in gedruckten oder elektronischen Verzeichnissen, die der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglich sind, zu informieren. Das gilt auch für weitere Nutzungsmöglichkeiten elektronischer Verzeichnisse aufgrund von Suchfunktionen.

(3) Der Endnutzer eines rufnummernabhängigen elektronischen Kommunikationsdienstes kann vom Anbieter jederzeit verlangen, mit seiner Rufnummer, seinem Namen, seinem Vornamen und seiner Anschrift in ein allgemein zugängliches, nicht notwendig anbietereigenes Endnutzerverzeichnis unentgeltlich eingetragen zu werden oder seinen Eintrag wieder löschen zu lassen. Einen unrichtigen Eintrag hat der Anbieter zu berichti-

gen. Die Ansprüche stehen auch Wiederverkäufern von rufnummernabhängigen elektronischen Kommunikationsdiensten für deren Teilnehmer zu.

§ 19

Bereitstellen von Endnutzerdaten

Der Anbieter eines rufnummernabhängigen elektronischen Kommunikationsdienstes hat jedem Unternehmen auf Antrag Endnutzerdaten nach § 18 Absatz 1 zum Zwecke der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten, Diensten zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers und Teilnehmerverzeichnissen zur Verfügung zu stellen. Die Überlassung der Daten hat unverzüglich und in nichtdiskriminierender Weise zu erfolgen. Die Daten müssen vollständig und inhaltlich sowie technisch so aufbereitet sein, dass sie nach dem jeweiligen Stand der Technik ohne Schwierigkeiten in ein kundenfreundlich gestaltetes Endnutzerverzeichnis oder eine entsprechende Auskunftsdienste-Datenbank aufgenommen werden können.

Teil 3

Telemediendatenschutz

§ 20

Technische und organisatorische Vorkehrungen

(1) Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Endnutzer ist über diese Möglichkeit zu informieren.

(2) Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Endnutzer anzuzeigen.

(3) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

§ 21

Verarbeitung zum Zweck des Jugendschutzes

Hat ein Diensteanbieter 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.

§ 22

Verarbeitung zum Zweck der Auskunftserteilung

(1) Auf Anordnung der zuständigen Stellen dürfen Anbieter von Telemedien (Diensteanbieter) im Einzelfall Auskunft über personenbezogene Daten, die zur Bereitstellung oder im Zuge der Inanspruchnahme von Telemedien erhoben wurden, erteilen, soweit dies

1. für Zwecke der Strafverfolgung,

2. zur Gefahrenabwehr durch die Polizeibehörden der Länder,

3. zur Erfüllung der gesetzlichen Aufgaben der Behörden der Zollverwaltung und der nach Landesrecht zuständigen Behörden zur Wahrnehmung ihrer Prüfungsaufgaben nach § 2 Absatz 1 und 3 des Schwarzarbeitsbekämpfungsgesetzes und zur Verhütung und Verfolgung von damit zusammenhängenden Straftaten und Ordnungswidrigkeiten

4. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder

5. zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

(2) Der Diensteanbieter darf darüber hinaus im Einzelfall Auskunft über bei ihm nach Absatz 1 vorhandene Daten erteilen, soweit dies zur Durchsetzung zivilrechtlicher Ansprüche wegen der Verletzung absolut geschützter Rechte aufgrund rechtswidriger Inhalte, die von § 1 Absatz 3 des Netzwerkdurchsetzungsgesetzes erfasst werden, erforderlich ist.

(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. 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 Diensteanbieter ist als Beteiligter zu dem Verfahren nach Absatz 3 hinzuzuziehen. Er darf den Nutzer über die Einleitung des Verfahrens unterrichten.

§ 23

Auskunftsverfahren

(1) Wer geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, darf die nach zu diesem Zweck erhobenen personenbezogenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt nicht für Passwörter und 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 personenbezogenen Daten dürfen auch an-

hand 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, soweit eine in Absatz 3 genannte Stelle dies unter Angabe einer gesetzlichen Bestimmung, die ihr eine Erhebung der in Ab-satz 1 in Bezug genommenen Daten erlaubt, in Textform im Einzelfall verlangt und dies zu einem der folgenden Zwecke erforderlich ist:

1. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten,

2. zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder

3. für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 und 4 genannten Stellen.

An andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen nicht in Textform gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die um Auskunft ersuchenden Stellen.

(3) Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;

2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;

3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst;

4. die Behörden der Zollverwaltung und die nach Landesrecht zuständigen Behörden, soweit die Datenerhebung zur Wahrnehmung ihrer Prüfungsaufgaben nach § 2 Absatz 1 und 3 des Schwarzarbeitsbekämpfungsgesetzes und für die Verhütung und Verfolgung von damit zusammenhängenden Straftaten und Ordnungswidrigkeiten erforderlich ist.

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

(5) Wer geschäftsmäßig Telemediendienste 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 und die weitere Bearbeitung des Verlangens darf erst nach einem positiven Prüfergebnis freigegeben werden.

§ 24

Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten

(1) Abweichend von § 23 darf derjenige, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, die erhobenen Passwörter und 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 Daten dürfen übermittelt werden:

1. an eine zur Verfolgung von Straftaten zuständige Behörde, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in Absatz 1 genannten Daten zur Verfolgung besonders schwerer Straftaten nach § 100b Absatz 2 der Strafprozessordnung erlaubt, nach Anordnung durch ein Gericht verlangt, oder

2. an eine für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständige Behörde, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in Absatz 1 genannten Daten und zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, nach Anordnung durch ein Gericht verlangt.

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

(3) Derjenige, der geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt, hat die zu beauskunftenden Daten unverzüglich, vollständig und unverändert 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 Telemediendienste 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 und die weitere Bearbeitung des Verlangens darf erst nach einem positiven Prüfergebnis freigegeben werden.

Teil 4

Ordnungswidrigkeiten, Strafvorschriften und Aufsicht

§ 25

Ordnungswidrigkeiten

(1) Für die Verhängung von Geldbußen findet Artikel 83 der Verordnung (EU) 2016/679 Anwendung.

(2) Artikel 83 Absatz 5 der Verordnung (EU) 2016/679 findet auf folgende Verstöße Anwendung:

1. gegen das Verbot der Verarbeitung und des Speicherns von Verkehrsdaten nach § 10 Absatz 1;

2. gegen das Gebot nach § 11 Absatz 2 und nach § 13 Absatz 4, Daten unverzüglich zu löschen;

3. gegen das Verbot nach § 13 Absatz 1, Daten für andere Zwecke zu nutzen;

4. gegen das Verbot der Verarbeitung und des Speicherns von Standortdaten nach § 14 Absatz 1 oder

5. gegen das Verbot der Verarbeitung der personenbezogenen Daten von Minderjährigen nach § 21.

(3) Artikel 83 Absatz 4 der Verordnung (EU) 2016/679 findet auf folgende Verstöße Anwendung:

1. gegen das Verbot nach § 9, ohne Einwilligung des Endnutzers Informationen auf dessen Endeinrichtungen zu speichern oder auf Informationen, die bereits in seinen Endeinrichtungen des Endnutzers gespeichert sind, zuzugreifen;

2. gegen die den Anbietern von elektronischen Kommunikationsdiensten bei der Mitteilung von Einzelverbindungsnachweisen obliegenden Pflichten nach § 12 oder

3. gegen Pflichten im Zusammenhang mit der Rufnummernunterdrückung und Anzeige nach § 16.

(4) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig,

1. entgegen § 23 Absatz 4 die dort genannten Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt oder

2. entgegen § 24 Absatz 3 die dort genannten Daten nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt.

Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

§ 26

Strafvorschriften

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

1. entgegen § 6 Satz 1 oder 2 eine Nachricht abhört oder in vergleichbarer Weise zur Kenntnis nimmt oder den Inhalt einer Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt oder

2. eine verbotene Telekommunikationsanlage entgegen § 7 in Deutschland herstellt oder auf dem Markt bereitstellt.

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

§ 27

Aufsicht, Aufgaben und Befugnisse

(1) Die Bundesnetzagentur und der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nehmen die ihr nach den nachfolgenden Absätzen zugewiesenen Aufgaben und Befugnisse wahr. Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zuständige Aufsichtsbehörde über die Einhaltung der in Teil 1 und 2 dieses Gesetzes enthaltenen Bestimmungen zum Schutz der personenbezogenen Daten natürlicher Personen. Die Bundesnetzagentur ist zuständige Aufsichtsbehörde über die Einhaltung der in Teil 1 und 2 dieses Gesetz enthaltenen Bestimmungen, soweit es sich dabei nicht um Bestimmungen zum Schutz der personenbezogenen Daten natürlicher Personen handelt.

(2) Die Aufsichtsbehörden können im Rahmen ihrer Zuständigkeit nach Absatz 1 Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften dieses Gesetzes sicherzustellen. Der Verpflichtete muss auf Anforderung der Aufsichtsbehörde die hierzu erforderlichen Auskünfte erteilen. Die Aufsichtsbehörde ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen.

(3) Darüber hinaus kann die Aufsichtsbehörde bei Nichterfüllung von Verpflichtungen aus diesem Gesetz den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden elektronischen Kommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(4) Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit dies die Kontrollen nach Absatz 2 erfordern.

Artikel 2

Änderung des Telekommunikationsgesetzes

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

1. In § 3 werden die Nummern 3, 5 und 30 gestrichen

2. Die §§ 45m, 47, 88-107 werden aufgehoben.

3. In § 115 wird Absatz 4 aufgehoben und der bisherige Absatz 5 wird Absatz 4.

4. § 148 wird aufgehoben.

5. § 149 wird wie folgt geändert:

   a) In Absatz 1 werden die Ziffern 15-18 aufgehoben.

   b) In Absatz 2 Nummer 3 wird die Angabe „16 bis 17a, 18,“ gestrichen.

   c) In Absatz 2 Nummer 4 wird die Angabe „15, 17c,“ gestrichen.

   d) In Absatz 2 Nummer 5 wird die Angabe „17b,“ gestrichen.

Artikel 3

Änderung des Telemediengesetzes

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist, wird wie folgt geändert:

Die §§ 11-16 werden durch folgenden § 11 ersetzt:

„§ 11 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer absichtlich entgegen § 6 Abs. 2 Satz 1 den Absender oder den kommerziellen Charakter der Nachricht verschleiert oder verheimlicht.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 2c Absatz 1 in Verbindung mit § 2b Absatz 1 Satz 2 und Absatz 2 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,

2. entgegen § 5 Abs. 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält oder

3. entgegen § 10a Absatz 1 oder § 10b Satz 1 ein dort genanntes Verfahren nicht, nicht richtig oder nicht vollständig vorhält.

(3) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.“

Artikel 4

Änderung der Strafprozessordnung

Die Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 12. Juni 2020 (BGBl. I S. 1247) geändert worden ist, wird wie folgt geändert:

1. In § 100g werden die Wörter „§ 96 Absatz 1 des Telekommunikationsgesetzes“ durch die Wörter „§ 10 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

2. In § 100j werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und Daten, die nach § 111 des Telekommunikationsgesetzes erhoben wurden“ ersetzt.

Artikel 5

Änderung des Bundesverfassungsschutzgesetzes

Das Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 16 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. In § 8a werden die Wörter „§ 96 Abs. 1 Nr. 1 bis 4 des Telekommunikationsgesetzes“ durch die Wörter „§ 10 Abs. 1 Nr. 1 bis 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

2. In § 8d werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

Artikel 6

Änderung des Urheberrechtsgesetzes

In § 101 des Urheberrechtsgesetzes vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 1 des Gesetzes vom 28. November 2018 (BGBl. I S. 2014) geändert worden ist, werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nr. 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien.)“ ersetzt.

Artikel 7

Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das durch Artikel 152 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. In § 10 werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „„Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

2. In § 40 werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

3. In § 52 werden die Wörter „(§ 96 Absatz 1 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 10 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt und die Wörter „(§ 15 Absatz 1 des Telemediengesetzes)“ gestrichen.

Artikel 8

Änderung des De-Mail-Gesetzes

Das De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 14 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist, wird wie folgt geändert:

1. In § 7 werden die Wörter „§ 47 des Telekommunikationsgesetzes“ durch die Wörter „§ 19 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

2. In § 15 werden die Wörter „Telemediengesetzes, Telekommunikationsgesetzes und Bundesdatenschutzgesetzes“ durch die Wörter „Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und Bundesdatenschutzgesetzes“ ersetzt.

Artikel 9

Änderung des BSI-Gesetzes

Das BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 73 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

In § 2 werden die Wörter „§ 3 Nummer 30 des Telekommunikationsgesetzes“ durch die Wörter „§ 2 Nr. 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“, die Wörter „Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes“ durch das Wort „Telemediennutzungsdaten“ und die Wörter „§ 88 Absatz 1 des Telekommunikationsgesetzes“ durch die Wörter „§ 4 Absatz 1 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

Artikel 10

Änderung des BND-Gesetzes

Das BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 19 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

In § 4 werden die Wörter werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

Artikel 11

Änderung des Zollfahndungsdienstgesetzes

Das Zollfahndungsdienstgesetz vom 16. August 2002 (BGBl. I S. 3202), das zuletzt durch Artikel 15 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202) geändert worden ist, wird wie folgt geändert:

1. In § 7 werden die Wörter werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

2. In § 15 werden die Wörter werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

Artikel 12

Änderung des MAD-Gesetzes

Das MAD-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2977), das zuletzt durch Artikel 18 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

In § 4 werden die Wörter werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

Artikel 13

Änderung des Wertpapierhandelsgesetzes

Wertpapierhandelsgesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2708), das zuletzt durch Artikel 4 des Gesetzes vom 27. März 2020 (BGBl. I S. 543) geändert worden ist, wird wie folgt geändert:

In § 7 werden die Wörter „§ 96 Absatz 1 des Telekommunikationsgesetzes“ durch die Wörter „§ 10 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

Artikel 14

Änderung des Einführungsgesetzes zur StPO

Das Einführungsgesetz zur Strafprozeßordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 312-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 4 des Gesetzes vom 27. März 2020 (BGBl. I S. 569) geändert worden ist, wird wie folgt geändert:

In § 12 werden die Wörter „§ 96 Absatz 1 des Telekommunikationsgesetzes“ durch die Wörter „§ 10 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

Artikel 15

Änderung des Patentgesetzes

Das Patentgesetz in der Fassung der Bekanntmachung vom 16. Dezember 1980 (BGBl. 1981 I S. 1), das zuletzt durch Artikel 4 des Gesetzes vom 8. Oktober 2017 (BGBl. I S. 3546) geändert worden ist, wird wie folgt geändert:

In § 140b werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nummer 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt.

Artikel 16

Änderung des Gebrauchsmustergesetzes

Das Gebrauchsmustergesetz in der Fassung der Bekanntmachung vom 28. August 1986 (BGBl. I S. 1455), das zuletzt durch Artikel 10 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2541) geändert worden ist, wird wie folgt geändert:

In § 24b werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nummer 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt.

Artikel 17

Änderung des Markengesetzes

Das Markengesetz vom 25. Oktober 1994 (BGBl. I S. 3082; 1995 I S. 156; 1996 I S. 682), das zuletzt durch Artikel 1 des Gesetzes vom 11. Dezember 2018 (BGBl. I S. 2357) geändert worden ist, wird wie folgt geändert:

In § 19 werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nummer 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt.

Artikel 18

Änderung des Designgesetzes

Das Designgesetz in der Fassung der Bekanntmachung vom 24. Februar 2014 (BGBl. I S. 122), das zuletzt durch Artikel 15 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2541) geändert worden ist, wird wie folgt geändert:

In § 46 werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nummer 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt.

Artikel 19

Änderung des Justizvergütungs- und entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 5 Absatz 2 des Gesetzes vom 11. Oktober 2016 (BGBl. I S. 2222) geändert worden ist, wird wie folgt geändert:

In Anlage 3 werden die Wörter „§ 3 Nr. 3 TKG“ durch die Wörter „§ 2 Nummer 4 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt

Artikel 20

Änderung des Versicherungsaufsichtsgesetzes

Das Versicherungsaufsichtsgesetz vom 1. April 2015 (BGBl. I S. 434), das zuletzt durch Artikel 6 des Gesetzes vom 19. März 2020 (BGBl. I S. 529) geändert worden ist, wird wie folgt geändert:

In § 305a werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nummer 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt.

Artikel 21

Änderung des Sortenschutzgesetzes

Das Sortenschutzgesetz in der Fassung der Bekanntmachung vom 19. Dezember 1997 (BGBl. I S. 3164), das zuletzt durch Artikel 6 Absatz 37 des Gesetzes vom 13. April 2017 (BGBl. I S. 872) geändert worden ist, wird wie folgt geändert:

In § 37b werden die Wörter „(§ 3 Nr. 30 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 2 Nummer 5 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)“ ersetzt.

Artikel 22

Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch Artikel 26 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

In § 22a werden die Wörter „Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten“ durch die Wörter „Auskunft über Bestandsdaten nach § 2 Nr. 4 des Gesetzes über den Datenschutz und den Schutz der

Privatsphäre in der elektronischen Kommunikation und bei Telemedien und nach § 111 des Telekommunikationsgesetzes erhobene Daten“ ersetzt.

Artikel 23

Änderung der Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), die zuletzt durch Artikel 27 des Gesetzes vom 20. November 2019 (BGBl. I S. 1724) geändert worden ist, wird wie folgt geändert:

1. In § 2 werden die Wörter „§ 96 des Telekommunikationsgesetzes“ durch die Wörter „§ 10 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

2. In § 35 wird die Angabe „§ 96“ durch die Wörter „§ 10 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien“ ersetzt.

Artikel 24

Änderung der Verordnung über Notrufverbindungen

Die Verordnung über Notrufverbindungen vom 6. März 2009 (BGBl. I S. 481), die zuletzt durch Artikel 1 des Gesetzes vom 26. November 2012 (BGBl. I S. 2347) geändert worden ist, wird wie folgt geändert:

1. In § 4 werden die Wörter „(§ 98 Absatz 3 des Telekommunikationsgesetzes)“ durch die Wörter „(§ 14 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien Gesetzes)“ ersetzt.

Artikel 25

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Mit dem Gesetzentwurf soll eine geschlossene und von den Bestimmungen des Telemediengesetzes und des Telekommunikationsgesetzes getrennte gesetzliche Reglung zum Datenschutz und zum Schutz der Privatsphäre geschaffen werden. Gesetzliche Anpassungen sind im Interesse der Rechtsklarheit erforderlich, da durch die Datenschutz-Grundverordnung (DSGVO) (Verordnung (EU) 2016/679) Bestimmungen zum Schutz der personenbezogenen Daten im Bereich des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) verdrängt werden und folglich nicht mehr anwendbar sind. Die Richtlinie 2002/58/EG in der durch die Richtlinie 2009/136/EG (E-Privacy-Richtlinie) geänderten Fassung ist weiterhin umzusetzen. Das derzeitige Nebeneinander von DSGVO, TMG und TKG führt zu Rechtsunsicherheiten bei Verbrauchern, die Telemedien und elektronische Kommunikationsdienste nutzen, bei Anbietern dieser Dienste und bei den Aufsichtsbehörden.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf enthält in Artikel 1 die zur Umsetzung der Richtlinie 2002/58/EG erforderlichen Bestimmungen, die derzeit im TKG enthalten sind. Die Datenschutzbestimmungen des TMG werden aufgehoben, soweit sie aufgrund des Vorrangs der Datenschutz-Grundverordnung nicht mehr anwendbar sind.

Das neue TTDSG (Artikel 1) enthält die Bestimmungen, die bisher in den §§ 88-107 TKG zur Umsetzung der Richtlinie 2002/58/EG enthalten waren, sowie weitere Bestimmungen, die bisher dort geregelt sind und die nicht durch die DSGVO ersetzt wurden. Es wird eine Rechtsgrundlage für die Anerkennung und Tätigkeit von Diensten zur Verwaltung persönlicher Informationen (Personal Information Management Services – PIMS) geschaffen. Weiterhin erfolgen Klarstellungen im Hinblick auf Endeinrichtungen, auf die aufgrund vertraglicher Vereinbarung oder gesetzlicher Anordnung zugegriffen werden darf. Die Aufsicht wird unter dem Gesichtspunkt neu gestaltet, dass zukünftig der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als unabhängige Datenschutzaufsichtsbehörde für die Aufsicht über die Bestimmungen zum Schutz der personenbezogenen Daten natürlicher Personen allein zuständig ist. Die Zuständigkeit der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) im Übrigen bleibt unberührt. Zudem werden die Datenschutzbestimmungen des TMG, soweit diese durch die DSGVO unberührt geblieben sind, im neuen TTDSG geregelt. Artikel 2 und 3 enthalten die Folgeänderungen durch Aufhebung der entsprechenden Bestimmungen im TKG und im TMG. Artikel 4 regelt das Inkrafttreten. Zieldatum ist der 21. Dezember 2020, der zugleich Stichtag für die Umsetzung der Richtlinie 2018/1972/EU ist und deren Anforderungen auch für die Umsetzung der Richtlinie 2002/58/EG gelten. Insbesondere die Begriffsbestimmungen der Richtlinie 2018/1972/EU finden auch auf die Bestimmungen zur Umsetzung der Richtlinie 2002/58/EG Anwendung.

III. Alternativen

Keine. Ein Verzicht auf die Regelung des Datenschutzes bei Telekommunikation und Telemedien ist im Hinblick auf die EU-Vorgaben nicht möglich. Die Regelung des Datenschutzes in einem neuen Stammgesetz außerhalb des TKG und des TMG soll erfolgen,

weil auch auf EU-Ebene die allgemeinen rechtlichen Rahmenbedingungen für die elektronischen Kommunikationsdienste und die Regelungen zum Datenschutz und zum Schutz der Privatsphäre nebeneinander bestehen und unabhängig voneinander fortentwickelt werden, z. B. im Rahmen der laufenden Verhandlungen zur E-Privacy-Verordnung.

IV. Gesetzgebungskompetenz

Die Gesetzgebungszuständigkeit des Bundes ergibt sich hinsichtlich der Bestimmungen zum Telekommunikationsdatenschutz aus der ausschließlichen Zuständigkeit für das Recht der Telekommunikation (Artikel 73 Absatz 1 Nummer 7 Grundgesetz). Die Regelung des Datenschutzes für den Bereich der Telemedien folgt aus der konkurrierenden Gesetzgebung des Bundes für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 Grundgesetz). Insoweit wird auf die Ausführungen zur Begründung der Gesetzgebungskompetenz im Gesetzentwurf der Bundesregierung zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (BT-Drs. 16/3078, S. 12) verwiesen.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Die im Gesetzentwurf enthaltenen Bestimmungen dienen der Umsetzung der Richtlinie 2002/58/EG, die bisher im TKG erfolgt, sowie der Anpassung der Datenschutzbestimmungen des TKG und des TMG an die Verordnung (EU) 20167679 (DSGVO).

VI. Gesetzesfolgen

Der Gesetzentwurf wirkt sich vor allem dahingehend aus, dass der Datenschutz und der Schutz der Privatsphäre in der Telekommunikation und bei Telemedien zukünftig einheitlich aus einem Stammgesetz heraus beurteilt und damit losgelöst von anderen Diskussionen im TMG und im TKG geregelt werden kann. Inhaltlich sorgt er im Hinblick auf das Verhältnis zur DSGVO und mit Blick auf die bisherigen Diskussionen zur Einwilligung bei Endeinrichtungen und zur unabhängigen Datenschutzaufsicht für Rechtsklarheit. Unbeabsichtigte Gesetzesfolgen sind nicht erkennbar.

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf bereinigt die Regelungen des TMG um diejenigen Bestimmungen, die aufgrund des Vorranges der DSGVO nicht mehr anwendbar sind. Er schafft eine einheitliche Aufsicht durch den oder die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit (BfDI), soweit durch öffentlich zugängliche elektronische Kommunikationsdienste, die in den Anwendungsbereich der Richtlinie 2002/58/EG fallen, personenbezogene Daten verarbeitet werden.

2. Nachhaltigkeitsaspekte

Regeln und Indikatoren der Nachhaltigkeitsstrategie sind nicht betroffen.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

4. Erfüllungsaufwand

Es entsteht kein Erfüllungsaufwand für Bürgerinnen und Bürger sowie kein über die bereits bestehenden Regelungen der DSGVO und zur Umsetzung der E-Privacy-Richtlinie hinausgehender Erfüllungsaufwand für die Wirtschaft.

Es entsteht Erfüllungsaufwand beim Bund dadurch, dass zukünftig bei der oder dem BfDI zusätzliche Aufgaben im Bereich der Aufsicht im Bereich der elektronischen Kommunikationsdienste erwachsen, zum einen dadurch, dass zukünftig auch nummernunabhängige interpersonelle Kommunikationsdienste zu beaufsichtigen sind, und zum anderen dadurch, dass bei der Aufsicht über die Bestimmungen zum Schutz der personenbezogenen Daten eine umfassende Tätigkeit der oder des BfDI als unabhängiger Datenschutzaufsichtsbehörde zu gewährleisten ist.

5. Weitere Kosten

Weitere Kosten für die Wirtschaft, Kosten für soziale Sicherungssysteme, Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Der Gesetzentwurf schafft Rechtsklarheit für Verbraucherinnen und Verbraucher bezüglich der Einwilligung in das Speichern und Abrufen von Informationen auf ihren Endeinrichtungen durch Dritte. Der Gesetzentwurf hat keine gleichstellungspolitischen oder demografischen Auswirkungen.

VII. Befristung; Evaluierung

Im Hinblick auf die notwendige Einhaltung der EU-Vorgaben, die durch diesen Gesetzentwurf erfolgt, besteht keine Befristung und kein Erfordernis zur Evaluierung.

B. Besonderer Teil

Zu Artikel 1 (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien)

Artikel 1 führt die Bestimmungen über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation, die bisher im TKG enthalten waren (§§ 88-107 TKG) und auch der Umsetzung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (E-Privacy-Richtlinie) dienten, in ein neues Stammgesetz über. Ebenso sollen die Datenschutzbestimmungen für Telemedien, die bisher in den §§ 11 ff. des TMG enthalten waren, zukünftig hier geregelt werden. Die Neuregelung trägt der Fortentwicklung des EU-Rechts im Bereich der elektronischen Kommunikation Rechnung. Bestimmungen zum Schutz der Endeinrichtungen dienen der Rechtsklarheit, insbesondere im Hinblick auf unterschiedliche Auffassungen zur Anwendung der EU-Vorgaben sowie im Hinblick auf das Internet der Dinge.

Die E-Privacy-Richtlinie ersetzte im Jahre 2002 die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation. Diese Ursprungsrichtlinie sollte der Digitalisierung der Telekommunikationsnetze, insbesondere der Einführung des diensteintegrierenden digitalen Telekommunikationsnetzes (ISDN) und digitaler Mobilfunknetze und den damit einhergehenden Herausforderungen an den Schutz personenbezogener Daten und der Privatsphäre der Nut-

zer gerecht werden. Die E-Privacy-Richtlinie verfolgt das Ziel, die Regelungen an die Entwicklungen der Märkte und Technologien für elektronische Kommunikationsdienste anzupassen, 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.

Die E-Privacy-Richtlinie wurde durch die Richtlinie 2009/136/EG zur Anpassung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste an die weitere Technologie- und Marktentwicklung geändert. Weiterhin hat die DSGVO Auswirkungen auf die Anwendung der Bestimmungen der Richtlinie. Die Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation ist ab dem 21. Dezember 2020 auch für den Anwendungsbereich der E-Privacy-Richtlinie maßgeblich.

Die Europäische Kommission hat am 16. Januar 2017 einen Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz der personenbezogenen Daten in der elektronischen Kommunikation (E-Privacy-Verordnung) vorgelegt. Ziel dieses Vorschlages ist – neben der Kohärenz zur DSGVO – die weitere Anpassung der Regelungen an wichtige technische und wirtschaftliche Entwicklungen auf dem Markt. Verbraucher und Unternehmen nutzen zunehmend neue Internetdienste, die eine interpersonelle Kommunikation ermöglichen, z. B. Voice-over-IP (VoIP-) Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste. Solche Over-the-Top-Kommunikationsdienste („OTT-Dienste“) wurden vom derzeitigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der E-Privacy-Richtlinie, nicht erfasst.

Die Kommission drängte auf zügige Verhandlung und Verabschiedung der neuen Verordnung, um eine enge Verzahnung mit der ab 25. Mai 2018 anwendbaren DSGVO zu erreichen. Die Bundesregierung verfolgt insgesamt das Ziel, ein hohes Schutzniveau für die Vertraulichkeit von Kommunikationsdaten bei der E-Privacy-Verordnung und zugleich Spielraum für Innovation und digitale Geschäftsmodelle zu erhalten. Eine Einigung im Hinblick auf dieses Ziel konnte im Rat bisher nicht erreicht werden. Derzeit lässt sich nicht abschätzen, ob und wann es zu einer Einigung kommt und wann die neuen Regelungen gegebenenfalls in Kraft treten.

Das Kernanliegen der Kommission, d. h. die Anwendung der E-Privacy-Regelungen auf die OTT-Dienste, ist jedoch bereits über Artikel 2 Nummer 4b und Nummer 7 der Richtlinie (EU) 2018/1972 erreicht. Denn diese legt bereits fest, dass die OTT-Dienste als nummernunabhängige interpersonelle Kommunikationsdienste in den Anwendungsbereich des Kodex fallen, dessen Anwendungsbereich ab dem 21. Dezember 2020 auch für die die E-Privacy-Richtlinie maßgeblich ist.

Die in Deutschland insbesondere im Hinblick auf das Setzen von Cookies umstrittene Frage der Umsetzung von Artikel 5 Absatz 3 der E-Privacy-Richtlinie soll mit diesem Gesetzentwurf geklärt werden. Der Bundesgerichtshof ist in seinem Urteil vom 28. Mai 2020 (I ZR 7/16 - Cookie-Einwilligung II) davon ausgegangen, dass die Gesetzeslage in Deutschland den Anforderungen der Richtlinie entspricht. Insbesondere erlaubt § 15 Absatz 3 Satz 1 TMG in seiner geltenden Fassung in europarechtskonformer Auslegung nicht den Einsatz von Cookies ohne Einwilligung des Nutzers zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung. Neben anderen Datenschutzbestimmungen des TMG wird auch § 15 Absatz 3, der die Verarbeitung von Nutzungsdaten für die Erstellung von pseudonymen Nutzerprofilen für diese Zwecke erlaubt, solange der Nutzer nicht widerspricht, wird durch die Bestimmungen der DSGVO verdrängt und ist aufzuheben.

Zu Teil 1 (Allgemeine Vorschriften)

Zu Teil 1 (Datenschutz und Schutz der Privatsphäre in der elektronischen Kommunikation)

Teil 1 regelt die allgemeinen Bestimmungen (Geltungsbereich des TTDSG und Begriffsbestimmungen)

Zu § 1 (Geltungsbereich)

Zu Absatz 1

Absatz 1 beschreibt den Anwendungsbereich des Gesetzes und orientiert sich am Wortlaut von § 91 Absatz 1 TKG. Die Regelung knüpft an Artikel 3 der E-Privacy-Richtlinie an, die für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen. Der beschriebene Geltungsbereich wird erweitern auf den Datenschutz bei Telemedien. Es wird klargestellt, dass die DSGVO im Übrigen unverändert bleibt.

Zu Absatz 2

Absatz 2 übernimmt unverändert den Wortlaut von § 91 Absatz 2 TKG.

Zu § 2 (Begriffsbestimmungen)

§ 2 regelt die für das TTDSG relevanten Begriffsbestimmungen. Dabei werden vorhandene Begriffsbestimmungen des TKG, der DSGVO, der Richtlinie 2018/1972/EU (Kodex für elektronische Kommunikation) und der Richtlinie 2008/63/EG (Endeinrichtungen) übernommen.

Zu § 3 (Anerkannte Dienste zur Verwaltung persönlicher Informationen)

§ 3 enthält erstmals einen regulatorischen Ansatz von Personal Information Management Services (PIMS), der sich auf die Wahrnehmung von Nutzerrechten nach dem TTDSG bezieht. Diese können dabei helfen, die Erfüllung der Anforderungen an den Datenschutz und den Schutz der Privatsphäre rechtssicher zu erleichtern. § 3 stellt klar, dass Endnutzer ihre Rechte über PIMS ausüben können, wenn diese anerkannt sind. Die Anerkennung (Absatz 3) soll durch den oder die BfDI erfolgen, um sicherzustellen, das die Anerkennung nach einheitlichen Maßstäben für Deutschland erfolgt. Der vorgeschlagene § 3 trägt der Forderung der Verbraucherverbände nach einem gesetzlichen Rahmen Rechnung. Dazu zählen die Anforderungen an Vereinbarungen, die Endnutzer mit PIMS treffen (Absatz 1), die Unabhängigkeit von wirtschaftlichen Interessen an der Verarbeitung von Daten und die Anforderungen an die Qualität und Zuverlässigkeit von PIMS. Diese sollen insbesondere durch ein Sicherheitskonzept nachweisen, dass zur Einhaltung der gesetzlichen Anforderungen an Datenschutz und Datensicherheit in der Lage sind (Absatz 2).

Zu § 4 (Vertraulichkeit der Kommunikation – Fernmeldegeheimnis)

§ 4 übernimmt die bisher in § 88 TKG enthaltene Regelung zum Fernmeldegeheimnis, die lediglich im Hinblick auf den Begriff der elektronischen Kommunikation redaktionell an die Begriffsbestimmung der E-Privacy-Richtlinie angepasst wird und sonst inhaltlich unverändert bleibt. Die Regelung konkretisiert das in Artikel 10 Grundgesetz (GG) enthaltene Fernmeldegeheimnis und setzt zugleich Artikel 5 Absatz 1 E-Privacy-Richtlinie um.

Zu § 5 (Verlangen eines amtlichen Ausweises)

§ 5 übernimmt die bislang in § 95 Absatz 4 TKG enthaltene Bestimmung. Die Regelung zur Vorlage eines Personalausweises und zur Anfertigung einer Kopie steht im Zusammenhang mit den Bestimmungen zu Personalausweisen und zur Identitätsfeststellung und wird von der DSGVO und der E-Privacy-Richtlinie nicht berührt. Die bisherige Regelung wird um die Möglichkeit des elektronischen Identitätsnachweises durch den Teilnehmer ergänzt. Nicht aufgenommen ist die bisher in § 95 Absatz 4 letzter Satz TKG enthaltene Regelung, wonach der Diensteanbieter nur Bestandsdaten verwenden darf, da insoweit wiederum die DSGVO zur Anwendung kommt.

Zu § 6 (Abhörverbot, Geheimhaltungspflicht der Betreiber von Funkanlagen)

§ 6 übernimmt die bislang in § 89 TKG enthaltene Bestimmung. Es erfolgt lediglich eine Anpassung an den Begriff der Funkanlagen nach dem Funkanlagengesetz, der die Empfangsanlagen (so der bisherige Wortlaut im TKG) umfasst. Die Regelung wird von der DSGVO und der E-Privacy-Richtlinie nicht berührt.

Zu § 7 (Missbrauch von Telekommunikationsanlagen)

Die Regelung übernimmt die bislang in § 90 TKG enthaltene Regelung, die im Wortlaut geringfügig angepasst wurde und Konkretisierungen zum Zweck der Klarstellung enthält. Die Regelung zielt darauf ab, das unbemerkte Abhören von Gesprächen und das unbemerkte Aufnehmen von Bildern zu verhindern, indem Produkte verboten werden, die hier eine besondere Gefahr begründen. Die Nutzung von versteckten Mikrofonen und Kameras in verschiedensten Produkten nimmt stetig zu, womit die Gefahren für die Privatsphäre sich verstärken. Besonders bei Alltagsgegenständen sollen die Nutzer und Dritte davor geschützt werden, dass sie unbemerkt abgehört werden oder unbemerkt Bilder von ihnen aufgenommen werden. Die Tätigkeit der Bundesnetzagentur zur Bekämpfung von sogenannten Spionagegeräten hat eine hohe Akzeptanz und ist weiterhin wichtig.

Zu Absatz 1:

Absatz 1 entspricht § 90 Absatz 1 TKG, knüpft im Wortlaut aber an den Sprachgebrauch im deutschen und europäischen Recht bei der Vermarktung von Produkten an. Der bisherige Bezug auf Sendeanlagen und sonstige Telekommunikationsanlagen wird durch den Begriff der Telekommunikationsanlagen ersetzt, der auch Sendeanlagen umfasst. Bereitstellen auf dem Markt ist jede entgeltliche und unentgeltliche Abgabe einer Funkanlage zum Vertrieb, zum Gebrauch oder zur Verwendung im Rahmen einer Geschäftstätigkeit (vgl. z. B. § 3 Nr. 9 Funkanlagengesetz).

Gegenstände des täglichen Gebrauchs sind Wirtschaftsgüter, die üblicherweise zur Nutzung angeschafft werden. Sie zeichnen sich dadurch aus, dass für ihre Nutzung keine besonderen Fachkenntnisse erforderlich sind, die nur einem begrenzten Expertenkreis zugänglich sind.

Verkleidet ist eine Telekommunikationsanlage iSd § 7 TTDSG mit einem Gegenstand des täglichen Gebrauchs stets dann, wenn sie von außen nicht ohne weiteres erkannt werden kann, sie somit als getarnt anzusehen ist. Unerheblich ist hierbei, ob der Gegenstand neben der Funktion, nach der er aussieht, noch weitere Funktionen besitzt. Es kommt darauf an, ob das unauffällige Aussehen der Telekommunikationsanlage, welches durch den Hersteller gewählt wurde, eine unbemerkte Aufnahme gerade durch das Zutun des Herstellers ermöglicht.

Eine Telekommunikationsanlage ist zur unbemerkten Aufnahme geeignet, wenn der Aufgenommene die Aufnahmesituation nicht unter Kontrolle hat. Ist der Nutzer selbst der Aufgenommene, muss er Kenntnis davon haben, dass die Telekommunikationsanlage Audio- oder Bilddateien an den Hersteller oder andere Unternehmen weiterleitet. Darüber

hinaus muss er bestimmen können, was von ihm aufgenommen wird. Hierzu gehört, dass er Einfluss darauf nehmen kann, ob eine Aufnahme gemacht wird, wann die Aufnahme beginnt und wann die Aufnahme endet. Erfolgt die Aufnahme eines Dritten durch den Besitzer der Telekommunikationsanlage, muss die Aufnahmesituation z. B. durch die Größe und Beschaffenheit der Telekommunikationsanlage oder durch optische oder akustische Signale für einen arglosen Dritten deutlich erkennbar sein.

Der Satz 2 dient der Klarstellung zum Tatbestandsmerkmal „bestimmt“. Damit werden bisherige Unklarheiten bei der Rechtsanwendung beseitigt. Wenn ein Hersteller eine Abhör- oder Bildaufnahmefunktion in einen Alltagsgegenstand integriert, gefährdet er die Privatsphäre eines Betroffenen und hat dafür Sorge zu tragen, dass mit diesem Gegenstand weder der Nutzer noch ein Dritter bei bestimmungsgemäßem Gebrauch unbemerkt aufgenommen wird. Hierbei ist der bestimmungsgemäße Gebrauch des Alltagsgegenstandes zu berücksichtigen sowie die Weite des Aufnahmewinkels oder die Reichweite des Mikrofons. Alltagsgegenstände, bei denen üblicherweise nicht davon ausgegangen wird, dass sie eine Kamera oder ein Mikrofon beinhalten, werden nicht so eingehend betrachtet wie neuartige Gegenstände. Daher ist es Aufgabe des Herstellers, den Gegenstand so zu gestalten, dass die Aufnahmesituation klar erkennbar wird und es dem Betroffenen so ermöglicht wird, diese zu unterbinden.

Grundsätzlich reicht ein Kamerasymbol zur Enttarnung nicht aus, da Alltagsgegenstände von arglosen Dritten regelmäßig nicht besonders betrachtet werden und somit das Kamerasymbol auch nicht wahrgenommen wird. Anders ist es bei Gegenständen, die die Aufmerksamkeit des arglosen Dritten auf sich ziehen, etwa wenn zusätzlich zum Kamerasymbol gut wahrnehmbare akustische oder visuelle Signale vom aufzeichnenden Gegenstand ausgehen. Dann kann der Betroffene nämlich das darauf angebrachte Kamerasymbol erkennen und eine Filmaufnahme von sich unterbinden. Eingesetzte Kamerasymbole müssen dann jedoch mit dem Gegenstand fest verbunden sein. Leicht ablösbare Aufkleber reichen hierfür nicht aus, da sie zum missbräuchlichen Einsatz des Gegenstandes durch Entfernen des Kamerasymbols einladen.

Zu Absatz 2:

Absatz 2 entspricht § 90 Absatz 2 TKG. Die bisherige Regelung nennt jetzt auch Bildung und Forschung als Grund für eine Ausnahmeregelung, um der der Forschungs- und Wissenschaftsfreiheit Rechnung zu tragen.

Zu Absatz 3:

Absatz 3 entspricht § 90 Absatz 3 TKG.

Zu Absatz 4:

Absatz 4 enthält die Befugnis zur Abfrage von personenbezogenen Daten von Käufern und Verkäufern und die Befugnis zur Übermittlung seitens der auskunftserteilenden Stelle.

Die Rechtsgrundlagen für Abfrage und Übermittlung der Daten werden somit im Einklang mit der Rechtsprechung des Bundesverfassungsgerichts in einer Norm zusammengefasst (vgl. BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Rn. 123). Diese Abfragemöglichkeit ist zu einer effizienten Verfolgung des unrechtmäßigen Besitzes oder des Vertriebes von verbotenen Telekommunikationsanlagen geboten.

Käuferdaten besitzen sowohl die Verkäufer als auch die Betreiber von Verkaufsplattformen. Verkaufsplattformen sind im Onlinehandel die Orte, an denen Waren angeboten werden.

Um gegen den durch den Vertrieb verursachten rechtswidrigen Besitz verbotener Sendeanlagen vorgehen zu können, ist die Bundesnetzagentur auf die Herausgabe der Käufer-

daten durch den Verkäufer oder im Onlinehandel zumeist auch durch die Verkaufsplattformbetreiber angewiesen.

Auch die Verkaufsplattformbetreiber verfügen häufig über die Käuferdaten. Gerade wenn Verkäufer ihren Sitz im Ausland haben und sich den Anordnungen der Bundesnetzagentur zur Weitergabe der Daten entziehen, sind die Plattformbetreiber die einzigen, die die Bundesnetzagentur bei einem wirksamen Vorgehen gegen den rechtswidrigen Besitz verbotener Sendeanlagen unterstützen können.

Zu § 8 (Nachrichtenübermittlungssysteme mit Zwischenspeicherung)

§ 8 übernimmt die bisher in § 107 TKG enthaltene Bestimmung, die lediglich redaktionell auf Anbieter elektronischer Kommunikationsdienste angepasst wird.

Zu § 9 (Einwilligung bei Endeinrichtungen)

Artikel 5 Absatz 3 der E-Privacy-Richtlinie verlangt von den Mitgliedstaaten, sicherzustellen, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. An die Stelle der Richtlinie 95/46/EG ist seit dem 25. Mai 2018 die DSGVO getreten. Verweise auf die Richtlinie 95/46/EG gelten als Verweise auf die Datenschutz-Grundverordnung, d. h. für die zu erteilenden Informationen und die Einwilligung sind Artikel 4 Nummer 11 und Artikel 7 der Datenschutz-Grundverordnung maßgeblich.

Die Anforderungen der Richtlinie in Artikel 5 Absatz 3 der E-Privacy-Richtlinie sind erfüllt, wenn die Mitgliedstaaten keine Regelungen erlassen, die in den Anwendungsbereich der E-Privacy-Richtlinie fallen, nach welchen die Speicherung von Informationen oder der Zugriff auf Informationen im Endgerät ohne Einwilligung erlaubt wird und die sich außerhalb des von Artikel 5 Absatz 3 der E-Privacy-Richtlinie gesetzten Rahmens bewegen.

In Deutschland erlaubt bisher das TMG die Verarbeitung von Nutzungsdaten, soweit dies für die Inanspruchnahme von Telemedien und deren Abrechnung erforderlich ist. Dazu zählen auch Tätigkeiten, die eine spätere Verarbeitung von personenbezogenen Daten vorbereiten, worunter das Speichern und der Abruf von Informationen von Endgeräten fällt, insbesondere das Setzen und das Auslesen von Cookies. Das TMG erlaubt demgemäß solche Tätigkeiten, die nach Artikel 5 Absatz 3 der E-Privacy-Richtlinie technisch erforderlich sind, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Für diese Tätigkeiten verlangt die Richtlinie keine Einwilligung, so dass das TMG den Anforderungen der Richtlinie entspricht.

In Deutschland bestehen darüber hinaus keine gesetzlichen Regelungen, die in den Anwendungsbereich der E-Privacy-Richtlinie fallen und die Speicherung und den Zugriff auf Endgeräte ohne Einwilligung des Nutzers oder Teilnehmers erlauben.

Im Hinblick auf unterschiedliche Auffassungen zum Anwendungsbereich der E-Privacy-Richtlinie im Allgemeinen und des Einwilligungserfordernisses in Artikels 5 Absatz 3 der E-Privacy-Richtlinie im Besonderen besteht hinsichtlich der Rechtmäßigkeit des Speicherns von Informationen in Endgeräten und des Zugriffs auf Informationen, die dort bereits gespeichert sind, Klarstellungsbedarf. Der Klarstellungsbedarf bezieht sich auf die

Frage, wann keine Einwilligung erforderlich ist, und darauf wie die Anforderungen, die die DSGVO an die Einwilligung stellt, im Rahmen von Artikel 5 Absatz 3 der E-Privacy-Richtlinie erfüllt werden können. Das Urteil des Europäischen Gerichtshofes in der Rechtssache C 673/17 (Planet49) ist einzubeziehen.

Zu berücksichtigen sind wirtschaftliche und technologische Entwicklungen, die der europäische Gesetzgeber bei Verabschiedung der speziell auf die Verwendung von Cookies fokussierten Richtlinienvorgaben möglicherweise nicht vor Augen hatte. Zu nennen sind das Internet der Dinge, die zunehmende Maschine-Maschine-Kommunikation, Industrie 4.0 und künstliche Intelligenz.

Ein wichtiges Beispiel sind Smartmeter und andere Geräte zur Versorgung mit Elektrizität, Gas, Wasser oder Wärme. Wenn diese an ein öffentliches elektronisches Kommunikationsnetz angeschlossen sind, handelt es sich um Endeinrichtungen im Sinne der Richtlinie 2008/63/EG. Das TTDSG stellt klar, dass auf diese zugegriffen werden darf, soweit dies zur Erfüllung von Verpflichtungen aus dem Recht der Union oder des Messstellenbetriebsgesetzes, zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich ist.

Ein weiteres Beispiel ist der Zugriff auf Endeinrichtungen des Endnutzers zur Ausführung sicherheitsrelevanter Funktionen und Software-Updates, etwa beim automatisierten und vernetzten Fahren, im vitalen Interesse des Betroffenen, in der Gesundheitsversorgung, in der Arbeitswelt, in der intelligenten und vernetzten Herstellung von Gütern und Dienstleistungen.

Zu Absatz 1

Absatz 1 stellt als Grundsatz klar, dass Dritte auf Endeinrichtungen des Endnutzers nur mit dessen Einwilligung zugreifen können, um dort Informationen zu speichern oder um dort gespeicherte Informationen auszulesen.

Die Richtlinie verwendet noch den Begriff der „Endgeräte“, der jedoch nicht legal definiert ist. Der Begriff der Endgeräte ist synonym zum Begriff der Endeinrichtung zu verstehen, wie er in der Richtlinie 2008/63/EG definiert ist. Entscheidendes Merkmal ist der direkte oder indirekte Anschluss an ein öffentlich zugängliches Kommunikationsnetz. Der Begriff ist unstrittig und wurde auch seitens der Kommission in ihrem Vorschlag für eine E-Privacy-Verordnung zugrunde gelegt. Einrichtungen, die nicht an ein öffentliches Kommunikationsnetz angeschlossen sind, fallen nicht unter Artikel 5 Absatz 3 der E-Privacy-Richtlinie und damit auch nicht unter § 9 TTDSG.

Absatz 1 bezieht sich auf Endeinrichtungen des Endnutzers. Die Richtlinie wendet sich noch an den Teilnehmer oder Nutzer. Teilnehmer ist nach den bisherigen Bestimmungen (§ 3 Nummer 20 TKG) jede natürliche oder juristische Person, die mit einem Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten einen Vertrag über die Erbringung derartiger Dienste geschlossen hat. Im EU-Recht findet sich der Begriff des Teilnehmers jedoch nicht. Die Richtlinie (EU) 2018/1972 stellt auf den Endnutzer ab. Das ist jede natürliche oder juristische Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst in Anspruch nimmt oder beantragt, ohne selbst ein öffentliches elektronisches Kommunikationsnetz oder einen öffentlich zugänglichen elektronischen Kommunikationsdienst bereitzustellen (Artikel 2 Nummer 13 und 14). Der Begriff des Teilnehmers ist im Nutzerbegriff enthalten. Auch die von der Kommission vorgeschlagene E-Privacy-Verordnung stellt auf den Begriff des Endnutzers ab.

Hinsichtlich der Einwilligung verweist die E-Privacy-Richtlinie auf die Anforderungen der seinerzeit noch geltenden allgemeinen Datenschutzrichtlinie 95/46/EG. Seit dem 25. Mai 2018 gelten die Anforderungen der DSGVO, d. h. Artikel 4 Nummer 11 und Artikel 7. Hierzu enthalten die folgenden Absätze Klarstellungen.

Zu Absatz 2

Absatz 2 nennt Ausnahmen vom Einwilligungserfordernis.

Unter Nummer 1 ist die in Artikel 5 Absatz 3 der E-Privacy-Richtlinie enthaltene Ausnahme aufgeführt, wenn die Tätigkeit technisch erforderlich ist, um eine Kommunikation zu übermitteln oder vom Endnutzer nachgefragte Telemedien bereitzustellen (der von der Richtlinie verwendete Begriff „Dienste der Informationsgesellschaft“ entspricht dem Begriff der Telemedien im deutschen Recht).

Nummer 2 stellt klar, dass keine Einwilligung des Endnutzers erforderlich ist, wenn der Endnutzer mit einem Anbieter im Zusammenhang mit der Erbringung von Dienstleistungen ausdrücklich vertraglich vereinbart hat, dass der Diensteanbieter dazu Informationen auf der Endeinrichtung des Endnutzer speichern und auf dort gespeicherte Informationen zugreifen kann. Hat sich der Endnutzer insoweit vertraglich verpflichtet, kann die datenschutzrechtliche Einwilligung nicht mehr zur Anwendung kommen. Andernfalls könnten Anbieter solcher Dienstleistungen keine zuverlässigen Verträge erhalten, da die Einwilligung nach Artikel 7 Absatz 3 DSGVO jederzeit widerrufen werden kann. Es ist davon auszugehen, dass die Richtlinie nicht dem Endnutzer einen anlasslosen Ausstieg aus vertraglichen Verpflichtungen in die Hand geben wollte.

Nummer 3 enthält eine entsprechende Klarstellung wie unter Nummer 2, wenn es sich um gesetzliche Verpflichtungen handelt. Legt der Gesetzgeber fest, dass der Endnutzer den Zugriff auf bestimmte Endeinrichtungen zu dulden hat, kann diese Duldungspflicht nicht von der jederzeit widerruflichen Einwilligung des Endnutzers abhängen.

Zu Absatz 3

Absatz 3 stellt bestimmte Anforderungen an die Wirksamkeit der Einwilligung die sich aus dem Urteil des Europäischen Gerichtshofes in der Rechtssache C-673/17 (Planet49) ergeben.

Zu Absatz 4

Absatz 4 nimmt Bezug auf Erwägungsgrund 66 der Richtlinie 2009/136/EG, durch die Artikel 5 Absatz 3 der E-Privacy-Richtlinie geändert wurde. Danach kann die Einwilligung auch durch die Nutzung entsprechender Einstellungen, die der Endnutzer in seinem Browser vornimmt, oder durch eine andere Anwendung erfolgen. Ziel ist die größtmögliche Nutzerfreundlichkeit: der Endnutzer sollte sein Recht auf einfachste Weise wahrnehmen können. Dies trägt dazu bei, dass kleine und mittlere Unternehmen und Start-ups im Online-Handel gegenüber den Anbietern mit großer Marktdominanz nicht benachteiligt werden. Neben Browsereinstellungen sind auch Online-Verfahren zum Einwilligungsmanagement – etwa über Datentreuhänder – denkbar.

Zu § 10 (Verkehrsdaten)

§ 10 übernimmt die bisher in § 96 TKG enthaltene Regelung zur Verarbeitung von Verkehrsdaten, die redaktionell angepasst wird aber ansonsten inhaltlich unverändert bleibt.

Zu 11 (Entgeltermittlung und Entgeltabrechnung)

§ 11 übernimmt die bisher in § 97 TKG enthaltene Regelung zur Verarbeitung von Verkehrsdaten zur Entgeltermittlung und Entgeltabrechnung, die redaktionell angepasst wird aber ansonsten inhaltlich unverändert bleibt.

Zu § 12 (Einzelverbindungsnachweis)

§ 12 übernimmt die bisher in § 99 TKG enthaltene Regelung.

Zu § 13 (Störungen von Telekommunikationsanlagen und Missbrauch von elektronischen Kommunikationsdiensten)

§ 13 übernimmt die bisher in § 100 TKG enthaltene Regelung. Die Regelung enthält in Absatz 4 einen zusätzlichen bisher nicht enthaltenen Aspekt. Der Diensteanbieter soll zukünftig auch die Möglichkeit haben, Verkehrsdaten zum Schutz seiner Endnutzer vor unerwünschter Kommunikation zu verarbeiten.

Zu § 14 (Standortdaten)

§ 14 übernimmt die bisher in § 98 TKG enthaltene Regelung

Zu § 15 (Mitteilen ankommender Verbindungen)

§ 15 übernimmt die bisher in § 101 TKG enthaltene Regelung

Zu § 16 (Rufnummernanzeige und -unterdrückung)

§ 16 übernimmt die bisher in § 102 TKG enthaltene Regelung

Zu § 17 (Automatische Anrufweiterschaltung)

§ 17 übernimmt die in § 103 TKG enthaltene Regelung.

Zu § 18 (Endnutzerverzeichnisse)

§ 18 übernimmt die in §§ 45m und 104 TKG enthaltene Regelung.

Zu § 19 (Bereitstellen von Endnutzerdaten)

§ 19 übernimmt die in § 47 TKG enthaltene Regelung.

Zu Teil 3 (Telemediendatenschutz)

Teil 3 enthält die Bestimmungen zum Telemediendatenschutz, die nicht durch die DSGVO verdrängt werden. Dabei handelt es sich um bestimmte technische und organisatorische Vorkehrungen, die Regelung der Verarbeitung von Minderjährigen nach den Vorgaben der Audiovisuelle-Mediendienste-Richtlinie, zum Zwecke der Auskunftserteilung und das Auskunftsverfahren.

Zu § 20 (Technische und organisatorische Vorkehrungen)

Zu Absatz 1

Absatz 1 enthält die bisher in § 13 Absatz 6 TMG enthaltene Regelung, die Telemedien-anbieter unter dem Gesichtspunkt der Datenvermeidung und Datenersparnis verpflichtet, ihre Dienste anonym oder pseudonym anzubieten.

Zu Absatz 2

Absatz 2 enthält die bisher in § 13 Absatz 5 TMG enthaltene Regelung.

Zu Absatz 3

Absatz 3 enthält die bisher in § 13 Absatz 7 TMG enthaltene Regelung.

Zu § 21 (Verarbeitung zum Zweck des Jugendschutzes)

§ 21 enthält die bisher in § 14a TMG enthaltene Bestimmung, die unverändert übernommen wird. (Die Vorschrift wird parallel zu dem bereits laufenden Gesetzgebungsvorhaben zur Umsetzung der AVMD-Richtlinie im TMG bereits aufgenommen, da mit einem Inkrafttreten dieser Bestimmung zeitlich vor dem Inkrafttreten des TTDSG gerechnet werden kann, vgl. BT-Drs. 19/20664)

Zu § 22 (Verarbeitung zum Zweck der Auskunftserteilung)

§ 22 enthält die bisher in § 14 Absatz 2 bis 5 enthaltene Regelung.

Zu § 23 (Auskunftsverfahren)

§ 23 enthält die bisher in § 15a TMG enthaltene Regelung (Anm.: wird durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität eingefügt, vgl. BT-Drs. 19/20163)

Zu § 24 (Auskunftsverfahren bei Passwörtern und anderen Zugangsdaten)

§ 24 enthält die bisher in § 15b TMG enthaltene Regelung (Anm.: wird durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität eingefügt, vgl. BT-Drs. 19/20163)

Zu Teil 4 (Ordnungswidrigkeiten, Strafvorschriften und Aufsicht)

Teil 4 regelt die Ordnungswidrigkeiten, die Strafvorschriften und die Aufsicht

Zu § 25 (Ordnungswidrigkeiten)

Zu Absatz 1

Absatz 1 stellt klar, dass die Verhängung von Geldbußen nach Maßgabe des Artikels 83 DSGVO erfolgt. Bislang regelt das TKG in § 149 Geldbußen gegen Verstöße gegen einzelne Bestimmungen im Datenschutzteil des TKG (§ 149 Absatz 1 Nummer 15 bis 18). Der Bußgeldrahmen orientiert sich gemäß § 149 Absatz 2 TKG an den bisher üblichen Regelungen. Nach Artikel 83 Absatz 1 DSGVO und Artikel 15a Absatz 1 der E-Privacy-Richtlinie müssen die Sanktionen wirksam, verhältnismäßig und abschreckend sein. Der Bußgeldrahmen für den sensiblen Bereich des Schutzes der Privatsphäre in der elektronischen Kommunikation kann nicht hinter den Maßgaben der DSGVO zurückbleiben und soll sich daher daran orientieren. Nach Artikel 83 Absatz 2 DSGVO muss die Aufsichtsbehörde bei der Festlegung von Bußgeldern bestimmte Maßgaben berücksichtigen (z. B. Art, Schwere und Dauer des Verstoßes, Vorsätzlichkeit oder Fahrlässigkeit, getroffene Maßnahmen zur Minderung des Schadens, Zusammenarbeit mit der Aufsichtsbehörde).

Zu Absatz 2

Absatz 2 bringt Artikel 83 Absatz 5 DSGVO auf diejenigen Bereiche zur Anwendung auf die Bereiche zur Anwendung, die Datenschutzbestimmungen enthalten, d. h. Geldbußen von bis zu 20 Millionen EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

Zu Absatz 3

Absatz 3 bringt Artikel 83 Absatz 4 DSGVO für diejenigen Bereiche zur Anwendung, die keinen Bezug zu Datenschutzbestimmungen haben, d. h. Geldbußen von bis zu 10 Millionen EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit er-

zielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist

Zu § 26 (Strafvorschriften)

Zu Absatz 1

Absatz 1 enthält die bislang in § 148 Absatz 1 TKG enthaltene Bestimmung. Während § 148 Absatz 1 Nr. 1 TKG unverändert übernommen wird, soll sich die Strafbarkeit im Hinblick auf Spionagegeräte (§ 6 – Verbotene Telekommunikationsanlagen) zukünftig nicht mehr auf den Besitz beziehen, sondern nur noch auf die Herstellung und das Bereitstellen auf den Markt beziehen. Dies dient der Rechtssicherheit von Verbrauchern, die ansonsten in den Anfangsverdacht einer Straftat geraten, wenn sie etwa im europäischen Ausland vernetzte EU-rechtskonforme Produkte legal erwerben.

Zu Absatz 2

Absatz 1 enthält die bislang in § 148 Absatz 2 TKG enthaltene Bestimmung, die unverändert übernommen wird.

Zu § 27 (Aufsicht, Aufgaben und Befugnisse)

Zu Absatz 1

Absatz 1 ordnet die bisherige zwischen der BNetzA und der oder dem BfDI geteilte Aufgabenwahrnehmung neu. Zukünftig soll die Aufsicht über den Schutz der personenbezogenen Daten durch BfDI erfolgen. Die Zuständigkeit der BNetzA im Übrigen bleibt unberührt.

Bisher ist nach § 116 TKG vorgesehen, dass die BNetzA die ihr nach dem TKG zugewiesenen Aufgaben und Befugnisse wahrnimmt. Dazu gehört nach § 115 Absatz 1 TKG die Sicherstellung, dass die in den §§ 88 bis 107 TKG enthaltenen Vorschriften eingehalten werden. Im Hinblick auf die Aufgabenwahrnehmung durch BfDI sieht § 115 Absatz 4 TKG bislang vor, dass die Datenschutzkontrolle durch BfDI erfolgt, soweit für die geschäftsmäßige Erbringung von elektronischen Kommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden. Der oder die BfDI richtet seine Beanstandungen an die BNetzA und übermittelt dieser nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.

Diese Vorgaben stehen im Einklang mit dem europäischen Recht. Nach Artikel 15a der E-Privacy-Richtlinie erfolgt die Durchsetzung der die Richtlinie umsetzenden Bestimmungen durch die Regulierungsbehörden, in Deutschland ist das die BNetzA. Zugleich weist Artikel 15 Absatz 3 der E-Privacy-Richtlinie der nach Artikel 29 der Richtlinie 95/46/EG eingesetzten Datenschutzgruppe die in Artikel 30 der Richtlinie 95/46/EG festgelegten Aufgaben im Hinblick auf die von der E-Privacy-Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation, wahr. Die Richtlinie 95/46/EG wurde durch die DSGVO aufgehoben. Artikel 94 Absatz 2 Satz 2 DSGVO bestimmt, dass Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten als Verweise auf den Europäischen Datenschutzausschuss nach der DSGVO gelten. Damit bestimmt Artikel 15 Absatz 3 der E-Privacy-Richtlinie, dass der Europäische Datenschutzausschuss gemäß der DSGVO seine Befugnisse gemäß Artikel 70 DSGVO bei der E-Privacy-Richtlinie im Hinblick auf den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation ausübt. Daraus folgt aber nicht zwingend, dass die Aufsicht durch die unabhängigen Aufsichtsbehörden gemäß der DSGVO zu erfolgen hat. Die E-Privacy-Richtlinie enthält insoweit keinen Verweis auf die Richtlinie 95/46/EG und damit auf die DSGVO. Zu beachten ist allerdings Artikel 8 der europäischen Grund-

rechtecharta. Artikel 8 Absatz 3 der Grundrechtecharta bestimmt, dass die Einhaltung der Vorschriften zum Schutz der personenbezogenen Daten von einer unabhängigen Stelle überwacht werden soll. Daraus folgt aber wiederum nicht zwingend, dass die Aufsicht voll umfassend entsprechend der DSGVO zu erfolgen hat. Die bisherige Datenschutzkontrolle durch BfDI gemäß § 115 Absatz 4 TKG entspricht den Anforderungen in Artikel 8 Absatz 3 der Grundrechtecharta.

Dennoch ist die Frage umstritten, ob die Wahrnehmung der Datenschutzaufsicht durch die BNetzA als Regulierungsbehörde im Verhältnis zur Zuständigkeit der unabhängigen Datenschutzaufsichtsbehörden gemäß DSGVO im Übrigen angemessen ist. Diese Frage ist auch Gegenstand der laufenden Verhandlungen zur E-Privacy-Verordnung. Die Bundesregierung hat sich im Zuge dieser Verhandlungen darauf verständigt, dass sich die Datenschutzaufsicht zukünftig an der DSGVO orientieren soll, soweit die Verarbeitung personenbezogener Daten betroffen ist.

§ 27 Absatz 1 trägt dem Rechnung, indem festgelegt wird, dass sowohl BfDI wie auch BNetzA die ihnen nach diesem Gesetz zugewiesenen Aufgaben und Befugnisse wahrnehmen. BfDI ist die zuständige Aufsichtsbehörde im Hinblick auf die Bestimmungen zum Schutz der personenbezogenen Daten, soweit natürliche Personen betroffen sind. Dies betrifft nicht die in § 17 enthaltenen Bestimmungen für Telemedienanbieter. Im Hinblick auf den Schutz der personenbezogenen Daten bei Telemedien erfolgt keine Regelung der Aufsicht, so dass hier wie bisher die Gesetzesausführung gemäß Artikel 83 Grundgesetz bei den Ländern liegt. Daraus ergibt sich, dass die BNetzA in ausschließlicher Zuständigkeit über die Einhaltung der §§ 4-8, 13-15 und 19 sowie der oder die BfDI in ebenfalls ausschließlicher Zuständigkeit über die Einhaltung der §§ 9-12 und § 16 wacht.

Zu Absatz 2

Absatz 2 enthält die gleiche Regelung wie § 115 Absatz 1 TKG, bezogen auf die zuständige Aufsichtsbehörde, d. h. je nach betroffener Regelung die BNetzA oder der oder die BfDI.

Zu Absatz 3

Absatz 3 enthält die § 115 Absatz 3 TKG entsprechende Bestimmung.

Zu Absatz 4

Absatz 4 enthält die § 115 Absatz 4 TKG entsprechende Bestimmung.

Zu Artikel 2 – 24

Bei den Artikel 2-24 handelt es sich um Folgeänderungen im TKG, im TMG und in anderen Gesetzen, die sich daraus ergeben, dass die Datenschutzbestimmungen des TKG und des TMG aus diesen Gesetzen herausgelöst und in das neue TTDSG überführt werden.

Zu Artikel 25 (Inkrafttreten, Außerkrafttreten)

Artikel 25 regelt das Inkrafttreten des Gesetzes am Tag nach seiner Verkündung.