INFO
05

Datenschutz und Tele-kommunikation

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Impressum

Herausgegeben von:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Graurheindorfer Straße 153, 53117 Bonn
Tel. +49 (0) 228 997799-0
E-Mail: poststelle@bfdi.bund.de
Web: www.bfdi.bund.de

Realisation: Appel & Klinger Druck und Medien GmbH

Stand: Januar 2024, 1. Auflage

Hinweise zur geschlechtergerechten Formulierung
in BfDI-Publikationen finden Sie hier:
www.bfdi.bund.de/geschlechtergerechte-sprache

Datenschutz und
Telekommunikation

BfDI – Info 5

Inhalt

Haben Sie Fragen, die in die Zuständigkeit einer Landesdatenschutzbehörde fallen? Zu den aktuellen Kontaktdaten geht's hier:

(QR-Code scannen oder klicken)

Vorwort

Telekommunikation ist der Taktgeber unserer digitalen Gesellschaft. Wir alle nutzen ständig das Handy, das Internet und Messenger-Dienste, um zu kommunizieren, zu informieren, aber auch um zu arbeiten.

Längst sind die Grenzen zwischen Arbeitszeit und Freizeit, zwischen dienstlicher und privater Nutzung unserer Kommunikationsmittel fließend.

Mit den Gesetzesnovellierungen Ende 2021, mit einer aktuellen Fassung des Telekommunikationsgesetzes (TKG) und dem neuen Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) wurden die datenschutzrechtlichen Regelungen weitgehend zusammengefasst und die europäische Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) umgesetzt. Hierbei wurde zudem die Zuständigkeit des BfDI für den Bereich Telekommunikation gebündelt und die aufsichtsbehördlichen Befugnisse gestärkt.

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

Datenschutz hat ein klares Ziel: Die Privatsphäre zu schützen! Ich freue mich, wenn sich Bürgerinnen und Bürger für dieses Thema interessieren und sich informieren. Diese Broschüre soll dabei unterstützen. Wegen der großen Nachfrage haben wir die Info 5 neu aufgelegt. Sie gibt einen Überblick über die wichtigsten Normen im Telekommunikationsbereich und erläutert diese.

Bonn, im Januar 2024

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

1 Überblick über anwendbare Vorschriften

Einführung

Unter Telekommunikation ist mittlerweile nicht mehr nur die klassische Telefonie (Festnetz- oder Mobilfunknetz), sondern auch Kommunikation über das Internet zu verstehen. Mit der Einführung des neuen Telekommunikationsgesetzes (TKG) am 1. Dezember 2021 wurde der Begriff der Telekommunikation weit gefasst. Dieser umfasst in einem funktionellen Sinn alle gewöhnlichen Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglichen (siehe im Einzelnen Definition nach § 3 Nr. 24 TKG). Darunter fallen also auch E-Mails, Voice-Over-IP und Videokonferenzen (sogenannte Over-the-top [OTT]-Anwendungen).

Telekommunikationsanbieter unterliegen zahlreichen gesetzlichen Regulierungen, die teilweise eine datenschutzrechtliche Schutzrichtung haben, bzw. dem Schutz der Privatsphäre der Endverbraucher dienen sollen, teilweise aber auch auf einen fairen Marktzugang, eine flächendeckende Versorgung, allgemeine Verbraucherrechte oder die Einhaltung von bestimmten technischen Sicherheitsstandards zielen. Entsprechend wird die Einhaltung der Regelungen nicht nur vom BfDI, sondern auch von der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) überwacht. Aus der Perspektive des Schutzes der Privatsphäre knüpfen die Sonderregelungen des Telekommunikationsrechts für die Datenverarbeitung an die Übertragung von Informationen mittels Signalen, sei es über

Telefonnetze, per Funk oder durch das Internet an. Die Privatheit von Gesprächen oder Nachrichten, die nicht persönlich stattfinden, bzw. elektronisch übermittelt werden, soll besonders geschützt werden, auch wenn ein Medium bzw. ein Dritter zwischengeschaltet wird.

Gleichzeitig gelten, sofern nicht die telekommunikationsrechtlichen Spezialregelungen vorgehen, grundsätzlich die allgemeinen Regeln der Datenschutz-Grundverordnung (DSGVO), die an die jeweils konkrete Verarbeitung personenbezogener Daten anknüpfen.

Die vorliegende Broschüre gibt einen Überblick über die für den Datenschutz im Bereich Telekommunikation wichtigsten Vorschriften und die Zuständigkeit des BfDI.

Gesetzliche Regelungen zum Schutz der Privatsphäre und dem Schutz der personenbezogenen Daten, die für den Bereich Telekommunikation relevant sind, finden sich sowohl im Grundgesetz (Art. 10 Abs. 1 GG) und in den allgemeinen datenschutzrechtlichen Regelungen der DSGVO als auch in den spezifischen Regelungen zur Telekommunikation wie etwa dem Telekommunikationsgesetz (TKG), dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), und den europarechtlichen Regelungen (wie etwa dem Europäischen Kodex für die elektronische Kommunikation und der E-Privacy-Richtlinie [E-Privacy-RL]). Ebenfalls zu beachten sind Gesetze, die die Möglichkeiten staatlicher Überwachung zur Strafverfolgung regeln, wie etwa das Strafgesetzbuch (StGB) und Strafprozessordnung (StPO).

1.1 Grundgesetz

Das Fernmeldegeheimnis ist nach Art. 10 Abs. 1 GG unverletzlich. Dieses Grundrecht schützt Sie davor, dass der Inhalt sowie die näheren Umstände Ihrer Telekommunikation staatlichen Stellen zur Kenntnis gelangen. Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden (Art. 10 Abs. 2 GG). Art. 10 GG regelt nur den Schutz des Fernmeldegeheimnisses im Verhältnis zwischen Bürgerin oder Bürger und Staat. Verpflichtete nach Art. 10 Abs. 1 GG sind damit alle staatlichen Stellen. Art. 10 GG hat jedoch keine unmittelbare Wirkung für den privaten Rechtsverkehr. Anbieter von Telekommunikationsdienstleistungen unterliegen aber dem für diesen Bereich ergänzend bestehenden Fernmeldegeheimnis nach § 3 Abs. 1, 3 TTDSG.

1.2 Datenschutz-Grundverordnung

Die europäische DSGVO schafft einen unionsweiten allgemeinen Rechtsrahmen für die Verarbeitung personenbezogener Daten. Sie regelt zentrale Grundsätze für die Verarbeitung personenbezogener Daten, die bei jeder Verarbeitung zu befolgen sind. Für weiterführende Informationen wird auf die Broschüre „Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Texte und Erläuterungen (Info 1) verwiesen.

Die Info 1 können Sie bestellen oder herunterladen:

(QR-Code scannen oder klicken)

Als allgemeiner Rechtsrahmen gilt die DSGVO auch für Anbieter öffentlich zugänglicher Kommunikationsdienste, allerdings nur, soweit die E-Privacy-RL (2002/58/EG) keine Regelungen trifft, die dasselbe Ziel verfolgen (Art. 95 DSGVO). Dies bedeutet also einen grundsätzlichen Vorrang des TTDSG und des TKG als Spezialgesetze gegenüber der DSGVO.

1.3 Telekommunikationsgesetz und Telekommunikation-Telemedien-Datenschutz-Gesetz

Durch die Novellierung von TKG und TTDSG im Dezember 2021 werden nunmehr sowohl der europäische Kodex für die elektronische Kommunikation (durch das TKG) als auch die E-Privacy-RL umgesetzt (im TTDSG und teilweise im TKG). Bezüglich der europäischen E-Privacy-Verordnung (E-Privacy-VO) verhandeln seit dem 20. Mai 2021 Vertretungen von Rat, Europäischem Parlament und Europäischer Kommission im sogenannten Trilog-Verfahren über die finale Version.

Sobald eine Einigung erzielt wurde, soll die E-Privacy-VO erst nach Ablauf einer zweijährigen Übergangsfrist gelten. Die E-Privacy-VO würde dann weite Teile des TTDSG insoweit ersetzen, als dort die E-Privacy-RL umgesetzt wird.

Das TKG soll in erster Linie durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation fördern und so angemessene Telekommunikationsdienstleistungen gewährleisten. Im zehnten Teil des Gesetzes (§§ 164 bis 190 TKG) befinden sich die Regelungen zur öffentlichen Sicherheit.

Im TTDSG werden nunmehr datenschutzrechtliche Regelungen aus dem alten TKG und dem alten Telemediengesetz (TMG) in einem Gesetz zusammengefasst. Die datenschutzrechtlichen Regelungen für die Telekommunikation finden sich in Teil 2 des TTDSG. Dort werden in §§ 3 bis 18 Regelungen zum Fernmeldegeheimnis (§ 3 TTDSG) und besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten getroffen.

Zum Verhältnis dieser Regelungen zu den allgemeinen Bestimmungen der DSGVO ist Art. 95 DSGVO zu beachten, so dass die Regelungen des TTDSG, soweit sie der Umsetzung der E-Privacy-RL dienen, grundsätzlich den Vorschriften der DSGVO als Spezialregelungen vorgehen.

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

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

- *Kundendatenauskunftsverordnung (KDAV) und Technische Richtlinie Automatisiertes Auskunftsverfahren (TR-AAV):*
  Hier werden die Anforderungen an die automatisierte Auskunft nach § 173 TKG geregelt.

Wesentliche Sicherheitsanforderungen für Telekommunikationsanbieter ergeben sich zudem aus dem Katalog von Sicherheitsanforderungen (§ 167 TKG).

1.4 Strafprozessordnung

Anbieter von Telekommunikationsdiensten sind grundsätzlich zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ausnahmen von diesem Grundsatz sind nur dann zulässig, wenn sie gesetzlich angeordnet sind. So finden sich bspw. in der StPO Rechtsgrundlagen für Strafverfolgungsbehörden, aufgrund derer die Telekommunikationsunternehmen die Überwachung der Telekommunikation zu ermöglichen haben (§ 100a StPO) oder Auskünfte, z. B. über die Bestandsdaten (§ 100j StPO) und die Verkehrsdaten (§ 100g StPO) erteilen müssen.

1.5 Abgrenzung zum Telemedienrecht

Für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach dem TKG oder Rundfunk nach § 2 des Medienstaatsvertrages sind (Telemedien) gilt das Telemediengesetz (TMG). Die datenschutzrechtlichen Regelungen für Telemedien finden sich ebenfalls im TTDSG und zwar dort im Teil 3. Die strengeren Anforderungen in Bezug auf die Datenverarbeitung der Verkehrsdaten und mit Blick auf das Fernmeldegeheimnis gelten nur für Telekommunikationsdienste.

2 Datenschutzrechtliche Grundlagen im Bereich Telekommunikation

2.1 Telekommunikations-Dienstleister

Gemäß § 3 Nr. 1 TKG ist „Anbieter von Telekommunikationsdiensten“ jeder, der Telekommunikationsdienste erbringt. Der Begriff „Telekommunikationsdienst“ ist funktional auszulegen und umfasst als Neuerung gegenüber dem alten Recht alle gewöhnlichen Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglichen, unabhängig vom jeweiligen technischen Übertragungsweg. Es wird also nicht mehr ausschließlich an eine Signalübertragung in einem bestimmten Kommunikationsnetz angeknüpft, sondern die Übertragung kann auch allgemein über das Internet erfolgen.

Telekommunikationsdienste sind gemäß § 3 Nr. 61 TKG definiert als „in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:

a. Internetzugangsdienste,

b. interpersonelle Telekommunikationsdienste und

c. Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.“

Diese Definition hat der deutsche Gesetzgeber wörtlich aus dem Europäischen Kodex für die elektronische Kommunikation („Kodex“) übernommen.

Der interpersonelle Telekommunikationsdienst gemäß vorangegangenem lit. b) wird nach § 3 Nr. 24 TKG definiert als ein „gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind“.

OTT-Dienste

Unter die Regelungen des TKG können auch elektronische Dienste über das Internet – die sogenannten „Over-the-top“-Dienste (OTT-Dienste) fallen – wie zum Beispiel Email-, Messengerdienste, aber auch Videokonferenzen.

Alle Telekommunikationsdienstleister sind verpflichtet, die besonderen Anforderungen des TKG und des TTDSG zu erfüllen.

Abgrenzung zum Telemediendienst

Bei der Übermittlung von Nachrichten über das Internet und beim Internetzugang selbst müssen die Telekommunikationsdienste nach TKG von Telemediendiensten abgegrenzt werden. Das Angebot des Internetzugangs als solches sowie die vorgenannten OTT-Dienste sind Telekommunikationsdienste, während die Anbieter der Inhalte, also z. B. die Anbieter von Webseiten, Telemedienanbieter sind.

2.2 Zuständigkeit des BfDI

§ 29 Abs. 1 TTDSG weist dem BfDI eine spezielle Zuständigkeit für die Aufsicht über datenschutzrechtliche Bestimmungen des TTDSG zu:

„Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen verarbeitet werden, ist

der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde."

In § 9 Abs. 1 Bundesdatenschutzgesetz (BDSG) wird allgemein eine Sonderzuständigkeit des BfDI für (Telekommunikations-)Unternehmen festgelegt, soweit diese für die geschäftsmäßige Erbringung von Telekommunikationsdienstleistungen Daten von natürlichen oder juristischen Personen verarbeiten und sich die Zuständigkeit nicht bereits aus § 29 TTDSG ergibt.

„Der BfDI ist zuständig für die Aufsicht über Unternehmen, soweit diese für die geschäftsmäßige Erbringung von Telekommunikationsleistungen Daten von natürlichen und juristischen Personen verarbeiten und sich die Zuständigkeit nicht bereits aus § 29 des TTDSG ergibt."

Es besteht daher eine grundsätzlich umfassende Sonderzuständigkeit des BfDI für Datenschutz im Bereich Telekommunikation.

Seit der Novellierung besteht nach § 29 Abs. 3 TTDSG die Befugnis des BfDI für den Verstoß gegen datenschutzrechtliche Vorschriften des Telekommunikationsrechts die allgemeinen Maßnahmen entsprechend Art. 58 DSGVO zu ergreifen.

Internationale Zuständigkeit des BfDI

Hinsichtlich der internationalen Zuständigkeit des BfDI ist nach dem jeweils anwendbaren Gesetz zu unterscheiden. Im Rahmen der DSGVO richtet sich die Zuständigkeit gemäß Art. 55 DSGVO nach dem jeweiligen Hoheitsgebiet. Hier besteht nach den Regelungen des Art. 3 DSGVO eine Zuständigkeit des BfDI, wenn die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung in Deutschland erfolgt oder, wenn Waren oder Dienstleistungen an Personen im Inland angeboten werden. Um widerstreitende Entscheidungen verschiedener gleichzeitig zuständiger europäischer Aufsichtsbehörden zu vermeiden, gilt nach Art. 56 DSGVO das Prinzip der Zuständigkeit der federführenden Aufsichtsbehörde (One-Stop-Shop-Prinzip).

One-Stop-Shop-Prinzip

Für Unternehmen ist bei grenzüberschreitenden Datenverarbeitungen nur die Aufsichtsbehörde an ihrem Hauptsitz zuständig. Dadurch haben sie einen zentralen Ansprechpartner. Gleichzeitig ist dabei aber auch gewährleistet, dass sich die von der Datenverarbeitung Betroffenen mit Beschwerden immer an die Datenschutzaufsichtsbehörde an ihrem Wohnsitz wenden können.

Soweit Vorschriften des TTDSG betroffen sind, regelt § 1 Abs. 3 TTDSG die Anwendbarkeit für „alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen“. Anders als nach der DSGVO gilt nicht das Prinzip der federführenden Aufsichtsbehörde.

2.3 Datenschutzrechtliche Verantwortlichkeit und Auftragsverarbeitung

Sowohl für die Frage der Zuständigkeit aber auch für die bestehenden datenschutzrechtlichen Verpflichtungen beteiligter Akteure ist die Bestimmung der datenschutzrechtlichen Verantwortlichkeit bedeutsam.

Aufgaben des Verantwortlichen

Die oder der datenschutzrechtlich Verantwortliche muss die Vorschriften der DSGVO und – wenn es sich um einen Telekommunikationsanbieter handelt – auch die speziellen datenschutzrechtlichen Regelungen des TTDSG und des TKG einhalten und ist darüber rechenschaftspflichtig. Ebenso ist sie oder er für die Gewährung der Betroffenenrechte verantwortlich.

Die Bestimmung der Verantwortlichkeit richtet sich nach den allgemeinen Prinzipien der DSGVO, die in der Leitlinie des Europäischen Datenschutzausschusses (EDSA) konkretisiert worden sind (Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbei-

ter“ in der DSGVO vom 7. Juli 2021). Die Festlegung erfolgt nach den tatsächlichen Umständen im Einzelfall und typischen Verpflichtungen, die sich aus gesetzlichen Vorschriften – hier also den Regelungen des TKG und des TTDSG – ergeben.

Aus Sicht des BfDI bedeutet dies als Grundprinzip für den Sonderbereich Telekommunikation, dass hier zwischen der Sphäre der Anwenderin oder des Anwenders von Telekommunikationsdiensten und der Sphäre der Anbieterin oder des Anbieters der Telekommunikationsdienstleistungen unterschieden werden muss. Jede Sphäre begründet ihre eigene datenschutzrechtliche Verantwortlichkeit für die jeweils dort verarbeiteten Daten. Versendet also bspw. ein Unternehmen eine E-Mail über einen E-Mail-Dienst, so ist das Unternehmen die verantwortliche Stelle für die personenbezogenen Daten, die mittels der E-Mail versendet werden sollen, während der E-Mail-Dienstleister datenschutzrechtlich verantwortlich ist für die Sphäre der telekommunikationsspezifischen Diensteerbringung.

Klassische Auftragsverarbeiter im Telekommunikationsmarkt sind insbesondere externe Callcenter und Dienstleister für technische Aufgaben.

2.4 Verschiedene rechtliche Ebenen im Telekommunikationsbereich

In der vernetzten Kommunikationswelt müssen die rechtlichen Ebenen im Zusammenhang mit Telekommunikationsdiensten und die jeweils betroffenen datenschutzrechtlichen Verantwortlichkeiten gedanklich voneinander getrennt werden, um das für den jeweiligen Bereich anwendbare Datenschutzrecht zu ermitteln. Dies ist insbesondere bei vernetzten Endgeräten und einer Kommunikation über das Internet relevant. Es kommt dann jeweils auf den konkreten Übertragungsweg und die technischen Details an. Typischerweise können die folgenden Ebenen unterschieden werden:

2.4.1 Beziehung Kunde und Telekommunikationsanbieter

Die klassische Telekommunikationsbeziehung besteht zwischen der Endkundin oder dem Endkunden und dem Telekommunikationsanbieter, wie etwa dem Mobilfunkanbieter. Der Mobilfunkanbieter

verarbeitet die Kundendaten für die vertragliche Beziehung nach den allgemeinen Grundsätzen der DSGVO; hier spricht man von den „Bestandsdaten“. Bei der Durchführung der Telekommunikationsleistung fallen zudem Daten mit Bezug auf den Übermittlungsvorgang selbst an, die nicht nur die anrufende Person, sondern auch die angerufene Person betreffen. Bei diesen Daten spricht man von „Verkehrsdaten“. Der Telekommunikationsanbieter muss für die Erbringung der Mobilfunkleistung die Spezialregelungen des TKG und des TTDSG erfüllen. Danach muss er bestimmte Sicherheitsanforderungen einhalten, darf Verkehrsdaten nur unter bestimmten Voraussetzungen verarbeiten, Auskünfte an Sicherheitsbehörden nur unter bestimmten Bedingungen erteilen und muss das Fernmeldegeheimnis beachten. Die vorliegende Broschüre beschäftigt sich schwerpunktmäßig mit diesem Kernbereich des Telekommunikationsrechts.

2.4.2 Beziehung Kunde und Anbieter des Endgeräts

Verwendet die Kundin oder der Kunde bspw. ein Smartphone, so werden durch den Geräte- oder Betriebssystemhersteller ebenfalls viele personenbezogene Daten verarbeitet. Der Gerätehersteller ist nach Art. 25 DSGVO zu einer datenschutzfreundlichen Technikgestaltung (privacy by design) verpflichtet. Außerdem muss er den Kunden möglichst datenschutzfreundliche Voreinstellungen anbieten (privacy by default). Im Übrigen sollte die Kundin oder der Kunde darauf achten, die Einstellungen ihres oder seines Geräts möglichst datenschutzsensibel vorzunehmen. Verwendet bspw. eine Endkundin das Gerät nicht privat, sondern in ihrer Funktion als Arbeitgeberin, so tritt eine weitere Ebene hinzu. Dann ist die Arbeitgeberin aus dem Arbeitsverhältnis heraus verpflichtet, bei den Einstellungen die Datenschutzrechte der Arbeitnehmerinnen und Arbeitnehmer zu wahren.

2.4.3 Beziehung Kunde und Anbieter von Telemedien

Nutzt die Kundin oder der Kunde über ihr oder sein Smartphone bestimmte Apps oder besucht Internetseiten, so verarbeiten die Anbieter der Apps oder der Internetseiten ihrerseits zahlreiche personenbezogene Daten. Diese Anbieter sind typischerweise keine Telekommunikationsanbieter, sondern Telemedienanbieter. Für diese sind daher die Vorschriften des TMG, des dritten Teils des TTDSG und die allgemeinen Vorschriften der DSGVO anwendbar.

2.5 Grundlagen der Datenverarbeitung

2.5.1 Bestandsdaten

Nach Art. 6 Abs. 1 DSGVO ist eine Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn es dafür eine Erlaubnis gibt. Eine Erlaubnis kann sich bspw. aus einem Gesetz ergeben, aus einem Vertrag oder aus einer Einwilligung der betroffenen Person.

Die Anbieter von Telekommunikationsdiensten erbringen ihre Dienste typischerweise innerhalb eines Vertragsverhältnisses. Sie dürfen daher nach Art. 6 Abs. 1 lit. b) DSGVO solche Daten verarbeiten, deren Verarbeitung für die Erfüllung dieses Vertrags erforderlich ist.

Außerdem dürfen gemäß Art. 6 Abs. 1 lit. f) DSGVO Daten verarbeitet werden, deren Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen der betroffenen Person am Schutz dieser Daten überwiegen.

Das TKG erlegt den Anbietern von Telekommunikationsdiensten zur Unterstützung von Polizei- und Strafverfolgungsbehörden umfangreiche Mitwirkungspflichten auf. Sofern in diesem Zusammenhang personenbezogene Daten gespeichert werden, die für das Vertragsverhältnis nicht erforderlich wären, ist die Verarbeitung gemäß Art. 6 Abs. 1 lit. c) DSGVO (Erfüllung einer rechtlichen Verpflichtung des Telekommunikationsanbieters) rechtmäßig.

Darüber hinaus ist für die Verarbeitung eine Einwilligung im Sinne von Art. 6 Abs. 1 lit. a) DSGVO erforderlich. Diese muss informiert und freiwillig erfolgen, darf nur auf bestimmte Verarbeitungszwecke bezogen sein und kann jederzeit widerrufen werden. Hier gelten die allgemeinen Grundsätze der DSGVO.

Zum praktisch häufigen Anwendungsfall der Werbung können Sie die Orientierungshilfe der Datenschutzkonferenz (DSK) zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung heranziehen (Stand Februar 2022).

Zur Orientierungshilfe geht's hier:

(QR-Code scannen oder klicken)

Einige Sachverhalte bei Bestandsdaten, z. B. zum Telefonbucheintrag, sind auch im TTDSG geregelt, so dass diese Regelungen gemäß Art. 95 DSGVO den allgemeinen Regelungen der DSGVO vorgehen.

2.5.2 Verkehrsdaten

Für die Verarbeitung der Verkehrsdaten, die im Zusammenhang mit der Erbringung des Telekommunikationsdienstes entstehen (§ 3 Nr. 70 TKG), wie etwa die Rufnummern, die IP-Adressen, der Zeitpunkt der Telekommunikation und bei mobilen Anschlüssen auch der Standort, gelten die Sonderregelungen des TKG und des TTDSG (vgl. § 9 TTDSG), die gemäß Art. 95 DSGVO den allgemeinen Regelungen der DSGVO vorgehen.

2.5.3 Steuerdaten

Für die Störungserkennung gibt es noch „Steuerdaten informationstechnischer Protokolle", die für diesen Zweck vergleichbar mit Verkehrsdaten verarbeitet werden dürfen.

2.6 Fernmeldegeheimnis

Das in § 3 TTDSG geregelte Fernmeldegeheimnis überträgt den grundrechtlichen Schutz des Art. 10 Abs. 1 GG, der lediglich die Bürgerinnen und Bürger vor Eingriffen des Staates schützt, auf das Verhältnis zwischen Privaten untereinander. Der Schutzbereich des § 3 TTDSG entspricht dem des Art. 10 Abs. 1 GG. Geschützt sind neben dem Inhalt der Kommunikation – und zwar unabhängig vom konkret genutzten

Kommunikationsmedium – auch deren nähere Umstände. Zu diesen näheren Umständen gehören:

- die von einem Anschluss aus gewählten Rufnummern, Kennungen und Zusatzdienste, auch wenn keine Verbindung zustande kommt,
- die Rufnummern oder Kennungen der Anschlüsse, die einen anderen Anschluss angerufen haben, auch wenn keine Verbindung zustande kommt,
- Informationen zur Um- und Weiterleitung von Telekommunikationsverkehren,
- bei Mobilfunkanschlüssen die Funkzellen, über die die Verbindung abgewickelt wird,
- Informationen zu dem jeweils in Anspruch genommenen Telekommunikationsdienst,
- Beginn und Ende der Verbindung oder des Verbindungsversuchs,
- Dauer der Verbindung.

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

Zur Wahrung des Fernmeldegeheimnisses verpflichtet sind nach § 3 Abs. 2 TTDSG

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürlich und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
2. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
3. Betreiber öffentlicher Telekommunikationsnetze und

4. Betreiber von Telekommunikationsanlagen, mit den geschäftsmäßig Telekommunikationsdienste erbracht werden.

Wegen des Fernmeldegeheimnisses dürfen auch die Anbieter von Telekommunikationsdiensten keine Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation erhalten, sofern dies nicht zwingend für die Erbringung des Dienstes erforderlich ist.

Eingriffe in das Fernmeldegeheimnis sind zulässig, wenn sie gesetzlich angeordnet sind. Die StPO (wie auch vergleichbare Regelungen) enthält Rechtsgrundlagen für Strafverfolgungsbehörden, aufgrund derer die Telekommunikationsdiensteanbieter die Überwachung der Telekommunikation zu ermöglichen haben (§ 100a StPO) oder Auskünfte, z. B. über die Verkehrsdaten (§ 100g StPO) erteilen müssen.

Verstöße gegen das Fernmeldegeheimnis

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

2.7 Typische Datenverarbeitungen durch Telekommunikationsanbieter

2.7.1 Bestandsdaten

Kundendaten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, bezeichnet das TKG als Bestandsdaten (§ 3 Nr. 6 TKG). Die Zulässigkeit der Verarbeitung der Bestandsdaten richtet sich im Wesentlichen nach der DSGVO.

2.7.2 Vertragsabschluss

Generell gilt: Der Diensteanbieter darf nur nach solchen Daten fragen, die für das Vertragsverhältnis erforderlich sind. Vor Vertragsabschluss darf nach dem Namen, dem Geburtsdatum, der Adresse und den Kontoverbindungsdaten gefragt werden. Bei im Voraus bezahlten Mobilfunkdiensten (Prepaid-Tarifen) ist der Diensteanbieter verpflichtet, die

Identität der Kunden zwecks etwaiger späterer Auskunftsersuchen der Sicherheitsbehörden zu überprüfen. Einige Daten zum Ausweisdokument muss er speichern (§ 172 Abs. 2 TKG).

Ist dagegen der Diensteanbieter vorleistungspflichtig, darf er die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Endnutzers erforderlich ist (§ 7 Abs. 1 TTDSG). Von dem Ausweis darf eine Kopie erstellt werden (vgl. hierzu und im Folgenden § 7 Abs. 3 TTDSG). Die Kopie ist unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Endnutzers zu vernichten. Andere als die für den Vertragsabschluss erforderlichen Daten dürfen dabei nicht verarbeitet werden. Hierbei ist darauf zu achten, dass nicht benötigte Angaben auf der Kopie des Ausweisdokuments geschwärzt werden.

Häufig wird bei Vertragsabschluss auch eine Prüfung der Kreditwürdigkeit (Bonitätsprüfung) durchgeführt; dabei werden die Daten an Auskunfteien übermittelt. Dies ist zulässig, wenn ein Postpaid-Vertrag abgeschlossen werden soll, der Diensteanbieter also in Vorleistung tritt und die Kundin oder der Kunde erst nach erhaltener Leistung zahlt. Der Diensteanbieter hat dann ein berechtigtes Interesse an der Anfrage bei einer Auskunftei (Art. 6 Abs. 1 lit. f) DSGVO). Die allgemeinen Grundsätze der DSGVO sind zu beachten. Bei Prepaid-Angeboten, bei denen der Diensteanbieter nicht in Vorleistung treten muss, findet eine Bonitätsprüfung in der Regel nicht statt und wäre datenschutzrechtlich auch nicht angezeigt.

2.7.3 Inkasso

Telekommunikationsdiensteanbieter machen offene Forderungen aus den Geschäftsbeziehungen mit ihren Kunden häufig nicht selbst geltend, sondern bedienen sich hierzu Inkassounternehmen. Zu diesem Zweck werden personenbezogene Daten der Kunden an das Inkassounternehmen übermittelt. Eine Übermittlung der zur Geltendmachung der Forderung erforderlichen personenbezogenen Daten ist unter den Voraussetzungen von Art. 6 Abs. 1 lit. f) DSGVO und § 10 Abs. 1 S. 3 TTDSG zulässig. Die Telekommunikationsdiensteanbieter haben ein berechtigtes Interesse an der Geltendmachung ihrer Forderungen. Auch die Geltendmachung rechtlich unsicherer Forderungen ist datenschutzrechtlich erlaubt. Ob die Telekommunikationsdiensteanbieter

die Forderungen selbst geltend machen oder hierzu auf ein nach dem Rechtsdienstleistungsgesetz (RDG) registriertes Inkassounternehmen zurückgreifen, ist ihre unternehmerische Entscheidung. Die Übermittlung personenbezogener Daten an Inkassounternehmen ist auch dann zulässig, wenn Kunden die Berechtigung der Forderung bestreiten.

Aus dem Beschluss des Bundesverfassungsgerichts (BVerfG) vom 14. August 2004 – 1 BvR 725/03 – wird allgemein geschlossen, dass die Beauftragung von Inkassounternehmen nicht nur mit schlichten Mahn- und Beitreibungstätigkeiten zulässig ist, sondern auch mit der Geltendmachung bestrittener Forderungen. Die Zulässigkeit der Übermittlung personenbezogener Daten an Inkassounternehmen hängt schließlich nicht davon ab, ob der Telekommunikationsdiensteanbieter die Erstattung der Kosten der Beauftragung des Inkassounternehmens von den Kunden verlangen kann.

Eingehendere Informationen zu diesem Thema sowie zu der Frage, unter welchen Voraussetzungen Forderungen bei Auskunfteien wie der Schufa eingemeldet werden dürfen, finden Sie in der Veröffentlichung „Datenverarbeitung in Inkassounternehmen – Antworten und häufig gestellte Fragen“ der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW)[1]. Weitere Hinweise zur Einmeldung von offenen und unbestrittenen Forderungen ergeben sich aus dem gleichnamigen Beschluss der DSK vom 23. März 2018[2],

Zu den FAQ der LDI NRW geht’s hier:

(QR-Code scannen oder klicken)

1 FAQ der LDI NRW, abrufbar unter: https://www.ldi.nrw.de/datenschutz/wirtschaft/inkasso
2 DSK Hinweise, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20180323_dskb_einmeldungen.pdf

Zu den Hinweisen der DSK geht's hier:

(QR-Code scannen oder klicken)

2.7.4 Löschung der Bestandsdaten

Der Diensteanbieter muss die Bestandsdaten löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Gespeichert werden die Bestandsdaten für den Kundensupport, die Rechtsabteilung, die Buchhaltung sowie für Auskunftsersuchen der Sicherheitsbehörden. Soweit die Speicherung ausschließlich aufgrund gesetzlicher Speicherpflichten erfolgt (§§ 238, 257 Handelsgesetzbuch [HGB], § 147 Abgabenordnung [AO], § 14b Umsatzsteuergesetz [UStG], § 172 TKG), hat nach Ablauf der dort normierten Fristen eine Löschung zu erfolgen. Im Übrigen erfolgt die Speicherung solange, wie der Diensteanbieter eine Erforderlichkeit nachweisen kann. In jedem Fall ist durch technische und organisatorische Maßnahmen sicherzustellen, dass nur diejenigen Personen auf die Daten zugreifen können, die einen solchen Zugriff auch benötigen. So benötigen etwa mehrere Jahre nach Vertragsbeendigung die Mitarbeiter des Kundensupports keinen Zugriff mehr auf Bestandsdaten, die ausschließlich zur Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten durch die Buchhaltung gespeichert werden dürfen.

2.7.5 Verkehrsdaten

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

Nach § 9 Abs. 1 TTDSG dürfen die in den Nummern 1 bis 5 konkretisierten Verkehrsdaten nur verarbeitet werden, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind die Verkehrsdaten nach Beendigung der Verbindung unverzüglich, also ohne schuldhaftes Zögern, zu löschen.

Die Verarbeitung von Verkehrsdaten ist außerdem zulässig für die folgenden Zwecke:

- Entgeltermittlung und Entgeltabrechnung (§§ 10, 11 TTDSG),
- Störungsbeseitigung und Missbrauchserkennung (§ 12 TTDSG),
- Vermarktung, bedarfsgerechte Gestaltung von Telekommunikationsdiensten und Bereitstellung von Diensten mit Zusatznutzen nach den Vorgaben des § 9 Abs. 2 TTDSG und
- Abrechnung der Telekommunikationsanbieter untereinander (siehe § 10 TTDSG).

Die Pflicht zur Verarbeitung von Verkehrsdaten aufgrund anderer Rechtsvorschriften bleibt nach § 9 Abs. 1 S. 4 TTDSG ebenfalls unberührt.

Zu den Speicherfristen für Verkehrsdaten finden sich im Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten weitergehende Informationen.[3]

Zum Leitfaden geht's hier:

(QR-Code scannen oder klicken)

3 Leitfaden von BfDI und BNetzA, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Themen/Telekommunikation/LeitfadenZumSpeichernVonVerkehrsdaten.html (www.bfdi.bund.de)

2.8 Technische und organisatorische Schutzmaßnahmen

Wer öffentliche Telekommunikationsdienste erbringt oder an der Erbringung dieser Dienste mitwirkt, z. B. durch Bereitstellung von Netzen, hat die ihm anvertrauten personenbezogenen Daten zu schützen und das Fernmeldegeheimnis zu wahren. Die für den Schutz erforderlichen technischen und sonstigen Maßnahmen werden durch das TKG und die DSGVO abstrakt umschrieben. Als Merksatz gelten für Verkehrsdaten die speziellen technischen Anforderungen gemäß § 165 TKG, während auf die Bestandsdaten die allgemeinen Regelungen nach Art. 32 DSGVO Anwendung finden.

Telekommunikationsdienstleister haben gemäß § 165 TKG erforderliche technische Vorkehrungen und sonstige Maßnahmen zu treffen, um den Schutz des Fernmeldegeheimnisses und der personenbezogenen Daten zu gewährleisten. Im Katalog von Sicherheitsanforderungen nach § 167 Abs. 1 TKG werden einige konkrete Anforderungen aufgeführt. Netzbetreiber und Erbringer von Diensten haben gemäß § 166 Abs. 1 Nr. 3 TKG ein Sicherheitskonzept zu erstellen, Netzbetreiber müssen dies auch der BNetzA vorlegen. Zu beachten ist, dass die Maßnahmen nach § 165 TKG auch, aber nicht ausschließlich dem Datenschutz dienen. Größere öffentlich zugängliche Telekommunikationsnetze werden als kritische Infrastruktur angesehen.

Kritische Infrastruktur

Kritische Infrastrukturen sind per Definition Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Insofern sind für diese Infrastrukturen bestimmte Maßnahmen umzusetzen, die zum Teil über den Anforderungshorizont des Datenschutzes hinausgehen können.

Die Maßnahmen müssen sowohl zum Zeitpunkt der Festlegung als auch zum Zeitpunkt der stattfindenden Verarbeitung die geforderten

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

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

2.9 Meldepflicht bei datenschutzrelevanten Datensicherheitsvorfällen und Schadsoftware

Anbieter öffentlich zugänglicher Telekommunikationsdienste müssen nach § 169 TKG und Art. 33 DSGVO Vorfälle melden bei denen der Schutz verarbeiteter personenbezogener Daten verletzt wurde. Diese gesetzliche Informationspflicht ist zweigliedrig ausgestaltet.

2.9.1 Meldung an die Aufsichtsbehörden

Eine Meldung muss – unabhängig von den Umständen des zu meldenden Vorfalls – im Fall des § 169 TKG nach der klaren gesetzlichen Vorgabe immer gegenüber der BNetzA und dem BfDI erfolgen. Fälle nach Art. 33 DSGVO sind nur an den BfDI zu melden. Für beide Fallkonstellationen stehen den Telekommunikationsdienstleistern entsprechende Meldeformulare zur Verfügung. Geringfügige Datenschutzverletzungen nach der DSGVO, die voraussichtlich nicht zu einem Risiko für die Betroffenen führen, müssen nicht gemeldet werden. Die Meldepflicht nach § 169 Abs. 1 S. 1 TKG gilt hingegen unbeschränkt, so dass auch vermeintlich kleinere Vorfälle mit potenziell weniger schweren Aus-

wirkungen den Aufsichtsbehörden mitzuteilen sind. BNetzA und BfDI haben für die Meldungen nach § 169 TKG gemeinsame Leitlinien für die Telekommunikationsdienstleister erstellt.

Hier geht's zum Artikel:

(QR-Code scannen oder klicken)

2.9.2 Benachrichtigung der Betroffenen

Neben der Meldung des Vorfalls an die Aufsichtsbehörden ist die umgehende Benachrichtigung der Betroffenen vorgesehen, sofern zu erwarten ist, dass diese hierdurch schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden (§ 169 Abs. 1 S. 2 TKG) bzw. die Datenschutzverletzung für diese voraussichtlich ein hohes Risiko zur Folge hat (Art. 34 DSGVO). Hierdurch sollen Betroffene in die Lage versetzt werden, eigene Schutzvorkehrungen zu treffen, um nachteilige Folgen der Datenschutzverletzung zu vermeiden oder zumindest begrenzen zu können. Die Benachrichtigung muss deshalb Informationen erhalten zu:

- der Art der Datenschutzverletzung,
- Kontaktpersonen oder -stellen, bei denen die Betroffenen weitere Informationen erhalten können,
- Empfehlungen und Maßnahmen, wie mögliche nachteilige Auswirkungen des Vorfalls begrenzt werden können.

Ausnahmsweise kann eine Benachrichtigung der Betroffenen entbehrlich sein, wenn die vom Datenschutzvorfall betroffenen Daten durch geeignete technische Vorkehrungen vor einer unberechtigten Kenntnisnahme geschützt sind, wie z. B. durch ein als sicher anerkanntes Verschlüsselungsverfahren. Soweit diese Vorfälle gegenüber den Aufsichts-

behörden meldepflichtig sind, prüfen diese, ob die Entscheidung, auf eine Benachrichtigung zu verzichten, rechtmäßig getroffen wurde und wirken andernfalls auf eine Nachholung der Benachrichtigung hin.

2.9.3 Verzeichnis der Datenschutzverletzungen

Neben der Melde- und Benachrichtigungspflicht des § 169 Abs. 1 TKG wird den Diensteanbietern in § 169 Abs. 3 TKG und Art. 33 Abs. 5 DSGVO auferlegt, ein Verzeichnis über die Vorfälle zu führen bzw. diese zu dokumentieren. Darin sind sämtliche Vorfälle aufzuführen und Angaben zu den Umständen und Auswirkungen der Verletzungen sowie zu den ergriffenen Abhilfemaßnahmen festzuhalten. Das Verzeichnis bzw. die Dokumentation müssen den Aufsichtsbehörden auf Anfrage zur Verfügung gestellt werden.

2.9.4 Schadsoftware

Diensteanbieter sind zudem verpflichtet ihre Nutzer darüber zu informieren, wenn sie feststellen, dass von deren Systemen Störungen ausgehen, die andere Telekommunikationsteilnehmer und eventuell sogar das Netz der Diensteanbieter beeinträchtigen. Dies kann bspw. der Fall sein, wenn ein Nutzer durch Schadsoftware auf seinem Computer Teil eines sogenannten „Botnetz“ geworden ist. Betroffene Computer können dann bspw. dazu verwendet werden, um ohne Wissen ihrer Besitzer Spam-E-Mails zu versenden oder andere Systeme anzugreifen. Die Diensteanbieter sind in diesen Fällen gehalten, ihren Nutzern neben der Information über die Störung im zumutbaren Rahmen auch Hinweise zu geben, wie diese bestmöglich behoben werden kann. Sofern es zum Schutz der Systeme des Diensteanbieters erforderlich ist, darf dieser zudem den betroffenen Nutzern so lange den Zugang zum Netz verwehren, bis diese die Störung auf ihren Systemen beseitigt haben. Die rechtlichen Grundlagen für dieses Vorgehen finden sich in § 169 Abs. 4 bis 7 TKG und § 12 TTDSG.

2.10 Betroffenenrechte

2.10.1 Information betroffener Personen nach Art. 13 und 14 DSGVO

Wenn personenbezogene Daten erhoben werden (also in der Regel beim Vertragsschluss), sind die hiervon betroffenen Personen nach

Art. 13 und 14 DSGVO zu informieren. Hierdurch soll die Transparenz der Datenverarbeitung sichergestellt werden.

Die Information muss umfassen:

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

Damit Betroffene wissen, wer die korrekte Ansprechperson im Unternehmen für datenschutzbezogene Anliegen ist, müssen auch die Kontaktdaten des/der betrieblichen Datenschutzbeauftragten mitgeteilt werden. Ferner muss auf bestehende Betroffenenrechte – etwa das Recht auf Berichtigung oder Löschung – sowie auf das Beschwerderecht bei der zuständigen Datenschutzbehörde hingewiesen werden.

2.10.2 Widerspruchsrecht

Unter den Voraussetzungen von Art. 21 DSGVO können Betroffene einer an sich rechtmäßigen Verarbeitung ihrer personenbezogenen Daten widersprechen. Hierauf sind sie von den Verantwortlichen hinzuweisen.

Bei Verarbeitungen zum Zwecke der Direktwerbung nach Art. 6 Abs. 1 lit. f) DSGVO besteht das Widerspruchsrecht voraussetzungslos.

2.10.3 Auskunftsanspruch betroffener Personen

Auch gegenüber Telekommunikationsanbietern besteht das allgemeine Auskunftsrecht nach Art. 15 DSGVO. Danach kann die betroffene Person von dem für die Datenverarbeitung Verantwortlichen Auskunft darüber verlangen, welche Daten dort über sie gespeichert sind bzw. verarbeitet werden. Außerdem erhält sie vom Verantwortlichen ergänzende Informationen, etwa über die Verarbeitungszwecke, die Herkunft der Daten, soweit diese nicht direkt bei ihr erhoben wurden, oder über Empfänger, an die ihre Daten übermittelt werden.

Das Recht auf Auskunft nach Art. 15 DSGVO wird aber nicht grenzenlos gewährt. Bei der Gewährung der Auskunft müssen z. B. gemäß Art. 15 Abs. 4 DSGVO die Rechte und Freiheiten anderer Personen beachtet werden. Damit werden in erster Linie die personenbezogenen Daten Dritter oder Betriebs- und Geschäftsgeheimnisse geschützt. Der Verantwortliche darf die Auskunft regelmäßig aber nicht vollständig verweigern, sondern muss bspw. die Namen dritter Personen in Dokumenten schwärzen, um ihre Identität nicht zu offenbaren. Einschränkungen sind ebenfalls hinsichtlich der Einzelverbindungsdaten wegen der Spezialregelung des § 11 TTDSG zu beachten. Diese Spezialregelungen gehen den allgemeinen Vorgaben der DSGVO vor, vgl. Art. 95 DSGVO.

2.10.4 Wie erhält man Auskunft?

Die Datenschutzerklärung der Telekommunikationsdiensteanbieter enthält üblicherweise Kontaktadressen, an die datenschutzrechtliche Anliegen wie der Auskunftsantrag adressiert werden können. Eine Auskunft ist prinzipiell formlos möglich. Bei telefonischen Auskunftsanträgen ist jedoch eine sichere Identifizierung meist nicht möglich, so dass Betroffene in diesen Fällen auf andere Kommunikationskanäle verwiesen werden können.

Tipps zur Auskunft

Es empfiehlt sich deshalb, die Auskunft von vornherein schriftlich oder elektronisch zu beantragen.
Im Auskunftsersuchen ist es ratsam, möglichst genau zu beschreiben, worüber man Auskunft wünscht. Dies erleichtert der verantwortlichen Stelle das Auffinden und die Zuordnung der Daten.

In der Praxis geht der Auskunftserteilung regelmäßig eine Legitimationsprüfung voraus, ob der Auskunftsantrag wirklich von der betroffenen Person gestellt wurde. Hierzu stellen Telekommunikationsdiensteanbieter den Antragstellenden üblicherweise einige Fragen zu den in der Kundendatenbank hinterlegten Daten, die in dieser Kombination ausschließlich von der Person beantwortet werden können, deren Identität bestätigt werden soll. Sofern um Übersendung einer Kopie eines amtlichen Lichtbildausweises gebeten wird und gute Gründe für die Vorlage einer solchen Ausweiskopie bestehen, werden regelmäßig nur Name, Anschrift, Geburtsdatum und Gültigkeitsdauer benötigt. Alle anderen auf dem Personaldokument befindlichen Daten (z. B. Ausweisnummer, Lichtbild, persönliche Merkmale, Staatsangehörigkeit) können auf der Kopie grundsätzlich geschwärzt werden. Die Daten auf der Ausweiskopie unterliegen zudem einer strengen Zweckbindung: Sie dürfen ausschließlich zur Identitätsprüfung verwendet werden, nicht aber in den Datenbestand der verantwortlichen Stelle einfließen. Zum eigenen Schutz sollten Ausweiskopien nicht per unverschlüsselter E-Mail versendet werden.

Sofern der Antrag elektronisch gestellt wird, ist der Verantwortliche verpflichtet, die Auskunft in einem gängigen elektronischen Format zu erteilen, sofern nicht ausdrücklich eine andere Form der Auskunftserteilung gewünscht wird.

Bei der Erteilung der Auskunft in elektronischer Form ist darauf zu achten, dass – in Abhängigkeit vom Schutzbedarf der Daten – bestimmte Datensicherheitsmaßnahmen getroffen werden sollten.

Die Auskunft ist innerhalb eines Monats zur Verfügung zu stellen, sofern die verantwortliche Stelle keine Gründe für eine Fristverlängerung

geltend machen kann, Art. 12 Abs. 3 DSGVO. In komplexen Fällen kann diese Frist um maximal weitere zwei Monate verlängert werden.

2.10.5 Was kostet eine Auskunft?

Grundsätzlich muss für die Auskunft nichts bezahlt werden. Etwas anderes gilt nur dann, wenn der Antrag offenkundig unbegründet oder – insbesondere im Fall häufiger Wiederholungen – exzessiv ist, was vom Verantwortlichen nachgewiesen werden muss. Für jede weitere Auskunft kann jedoch ein angemessenes Entgelt verlangt werden. Das geforderte Entgelt darf nicht höher sein als die entstandenen direkt zurechenbaren Kosten. Aber auch bei derartigen Auskünften muss nichts bezahlt werden, wenn besondere Umstände dafürsprechen, dass Daten unrichtig oder unzulässig gespeichert sind oder sich dies aus der Auskunft ergibt. Entsprechendes gilt, wenn eine Kopie der personenbezogenen Daten verlangt wird, die Gegenstand der Verarbeitung sind.

2.10.6 Recht auf Löschung

Die DSGVO schließt ein Recht auf Vergessenwerden ein. Nach Art. 17 Abs. 1 S. 1 DSGVO kann die betroffene Person von dem Verantwortlichen verlangen, die sie betreffenden personenbezogenen Daten unverzüglich zu löschen. Aus dieser Norm leitet sich also ein direkter Anspruch ab. Spiegelbildlich hierzu ist im zweiten Halbsatz von Art. 17 Abs. 1 DSGVO eine Löschpflicht vorgesehen, so dass der Verantwortliche auch antragsunabhängig verpflichtet ist, personenbezogene Daten unverzüglich zu löschen, sofern insbesondere einer der in Art. 17 genannten Gründe zutrifft. Zu beachten ist jedoch, dass eine Löschung nicht verlangt werden kann, wenn eine Verarbeitung aus anderen Gründen noch erforderlich ist, z. B. für die Vertragsabwicklung oder aber aus gesetzlichen Regelungen eine Aufbewahrungspflicht für den Verantwortlichen besteht (Art. 17 Abs. 3 DSGVO).

2.11 Beschwerderecht beim BfDI und dessen Befugnisse

Sieht eine betroffene Person bei einer Verarbeitung ihrer personenbezogenen Daten durch einen Telekommunikationsdienstleister im Sinne des TKG im Rahmen seiner geschäftsmäßigen Erbringung von Telekommunikationsdienstleistungen (§ 29 TTDSG) einen Verstoß

gegen datenschutzrechtliche Vorschriften der DSGVO (sofern nicht nach Art. 95 DSGVO durch Spezialregelungen verdrängt) oder der telekommunikationsspezifischen Datenschutzvorgaben, so steht ihr das Beschwerderecht beim BfDI nach Art. 77 DSGVO zu.

Der BfDI kann bei tatsächlichem Vorliegen eines Verstoßes Maßnahmen nach Art. 58 DSGVO (ggf. in Verbindung mit § 29 Abs. 3 TTDSG) gegenüber dem Telekommunikationsanbieter ergreifen.

Der BfDI hat damit gegenüber dem vorangegangenen Telekommunikationsrecht, wo er bei einem Verstoß gegen datenschutzrechtliche Bestimmungen des TKG nur Beanstandungen an die BNetzA melden konnte, stärkere eigene Befugnisse.

Hinweis

Es bleibt zu beachten, dass die Vorschriften des TTDSG und des TKG nicht ausschließlich datenschutzrechtliche Vorschriften sind. Entsprechend grenzt § 29 Abs. 1 TTDSG die Zuständigkeit des BfDI auf die Aufsicht über die Verarbeitung von (personenbezogenen) Daten von natürlichen oder juristischen Personen ein. Im Übrigen ist gemäß § 30 TTDSG die BNetzA die zuständige Aufsichtsbehörde für Telekommunikationsanbieter.

2.12 Übermittlung personenbezogener Daten an Drittländer

Datenübermittlungen zwischen den EU-Mitgliedstaaten und den Vertragsstaaten des Europäischen Wirtschaftsraums (EWR) im Anwendungsbereich der DSGVO sind datenschutzrechtlich genauso zu behandeln wie inländischer Datenverkehr. Für Datenübermittlungen an Drittländer außerhalb der EU und des EWR müssen zusätzlich die besonderen Bedingungen des Kapitels V der DSGVO erfüllt sein.

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

- Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 DSGVO)
  Mit dem sogenannten Angemessenheitsbeschluss stellt die Europäische Kommission fest, dass ein Drittland ein angemessenes Datenschutzniveau bietet. Derzeit bestehen Angemessenheitsbeschlüsse für folgende Länder: Andorra, Argentinien, Färöer, Guernsey, Israel, Isle of Man, Japan, Jersey, Kanada, Neuseeland, Uruguay, Republik Korea (Südkorea), die Schweiz und das Vereinigte Königreich (seit dem 28. Juni 2021, befristet bis 27. Juni 2025 mit Verlängerungsoption bei dann noch bestehendem angemessenem Schutzniveau). Seit dem 10. Juli 2023 gilt zudem der Angemessenheitsbeschluss für die USA (nur für US-Organisationen, die gemäß des EU-U.S. Data Privacy Framework zertifiziert sind). Die Anwendungsbereiche der jeweiligen Angemessenheitsbeschlüsse sind zu beachten. Die Angemessenheitsbeschlüsse, die die Europäische Kommission vor dem Geltungsbeginn der DSGVO getroffen hat, bleiben so lange in Kraft, bis sie durch einen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden (Art. 45 Abs. 9 DSGVO). Von dieser Möglichkeit hat die Kommission bisher keinen Gebrauch gemacht.

- Datenübermittlung auf Basis geeigneter Garantien (Art. 46 DSGVO)
  Falls kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, dürfen Übermittlungen personenbezogener Daten an Drittländer nur auf Basis sogenannter „geeigneter Garantien“ im Sinne des Art. 46 DSGVO erfolgen. Zu Letzteren gehören u. a. genehmigte verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCR) oder Standarddatenschutzklauseln der Europäischen Kommission (Standard Contractual Clauses – SCC). Im Fall der Standarddatenschutzklauseln bedarf es keiner gesonderten Genehmigung durch eine Aufsichtsbehörde (vgl. Art. 46 Abs. 2 lit. c) DSGVO). Des Weiteren können geeignete Garantien auch in individuellen Verträgen bestehen, die allerdings einer Genehmigung durch die zuständige Aufsichtsbehörde bedürfen (Art. 46 Abs. 3 lit. a) DSGVO). Daneben bestehen weitere geeignete Garantien, u. a. für den öffentlichen Bereich (Art. 46 Abs. 2 lit. a) und Abs. 3 lit. b) DSGVO).

→ Ausnahmen (Art. 49 DSGVO)
Falls weder ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt noch geeignete Garantien nach Art. 46 DSGVO bestehen, kommt eine Datenübermittlung an ein Drittland nur ausnahmsweise auf Basis von Art. 49 DSGVO in Betracht, z. B. dann, wenn die betroffene Person in die Datenübermittlung ausdrücklich eingewilligt hat oder die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist. Die Ausnahmevorschriften des Art. 49 DSGVO sind grundsätzlich eng auszulegen und dürfen nicht genutzt werden, um die Schutzvorschriften des Kapitels V zu umgehen (s. Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der Verordnung 2016/679).

EU-U.S. Data Privacy Framework

Mit der Annahme des Angemessenheitsbeschlusses zum sogenannten EU-U.S. Data Privacy Framework (EU-U.S. DPF) durch die Europäische Kommission am 10. Juli 2023 besteht wieder eine Übermittlungsgrundlage gemäß Art. 45 DSGVO für Datenübermittlungen an im Rahmen des EU-U.S. DPF zertifizierte Unternehmen in den USA. Im Jahr 2020 hatte der EuGH mit dem sogenannten Schrems II-Urteil (Urteil des EuGH vom 16. Juli 2020, Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems, [C-311/18, ECLI:EU:C:2020:559], die Vorgängerregelung, das „EU-U.S. Privacy Shield", für ungültig erklärt.

Zu beachten ist, dass es sich bei dem Angemessenheitsbeschluss zum EU-U.S. DPF um einen sektoralen Angemessenheitsbeschluss handelt und nicht um einen Angemessenheitsbeschluss für die gesamten USA. Das bedeutet, dass der Beschluss als Übermittlungsgrundlage nur für Datenübermittlungen an Unternehmen oder sonstige Organisationen in den USA gilt, die nach den Kriterien des EU-U.S. DPF zertifiziert sind.

In der Praxis erfolgt dies durch Selbstzertifizierung des Unternehmens oder der Organisation und Auflistung sowie Veröffentlichung in der vom U.S. Department of Commerce geführten „DPF"-Liste.

Für Datenübermittlungen aus der EU und dem EWR an die USA auf Grundlage des EU-U.S. DPF sind daher in dessen Anwendungsbereich keine zusätzlichen Übermittlungsinstrumente gemäß Art. 46 DSGVO oder zusätzlichen Maßnahmen mehr erforderlich. Einen praxisorien-

tierten Überblick über den Angemessenheitsbeschluss und zu Fragen des Anwendungsbereichs bieten die Anwendungshinweise der DSK.

Zu den Anwendungshinweisen der DSK geht's hier.

(QR-Code scannen oder klicken)

Für Drittländer, für welche kein Angemessenheitsbeschluss der Europäischen Kommission gilt, sind die Anforderungen des Schrems II-Urteils weiterhin relevant. Das bedeutet, dass im Falle der Verwendung von Übermittlungsinstrumenten gemäß Art. 46 DSGVO (wie z. B. Standardvertragsklausen oder BCR) im Rahmen des sogenannten „Transfer Impact Assessments" (TIA) geprüft werden muss, ob das verwendete Übermittlungsinstrument ausreichenden Schutz bietet oder ggf. durch zusätzliche technische oder organisatorische Schutzmaßnahmen gesichert werden muss. Bspw. dann, wenn die Annahme besteht, dass Behörden im Drittland auf übermittelte Daten zugreifen können. Der EDSA hat Empfehlungen für Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten veröffentlicht.

3 Praxisfragen von A bis Z

3.1 Arbeitgeber und Telekommunikationsdienste

Unternehmen und Behörden haben oftmals eigene Telekommunikations- und Computeranlagen, in denen sie mehrere Endgeräte wie Telefone und PCs miteinander verbinden, um sowohl interne als auch externe Kommunikation zu ermöglichen.

Das Unternehmen bzw. die Behörde muss dann die notwendigen technischen und organisatorischen Maßnahmen für einen sicheren Betrieb gewährleisten und sollte sich hierzu am IT-Grundschutz-Kompendium und den Bausteinen des BSI orientieren.

Zudem sind mit Blick auf die Arbeitnehmerinnen und Arbeitnehmer besondere Datenschutzregeln zu beachten. So sollte insbesondere bei der Einstellung der Anruflisten oder auch bei Präsenzinformationen auf möglichst datenschutzfreundliche Einstellungen geachtet werden.

Ob ein Unternehmen, wenn es eigene Kommunikationssysteme betreibt, auch als Anbieter eines Telekommunikationsdienstes im Sinne des § 3 TKG anzusehen ist und die Verpflichtungen des TKG beachten muss, hängt von der konkreten Ausgestaltung ab.

3.2 Einzelverbindungsnachweis

Kunden können nach § 65 TKG grundsätzlich von ihrem Anbieter öffentlich zugänglicher, nummerngebundener, interpersoneller Telekommunikationsdienste und von dem Anbieter von Internetzugangsdiensten mit Wirkung für die Zukunft eine nach Einzelverbindungen aufgeschlüsselte Rechnung (Einzelverbindungsnachweis) verlangen,

die zumindest die Angaben enthält, die für eine Nachprüfung der Teilbeträge der Rechnung erforderlich sind.

Gemäß § 11 Abs. 1 S. 4 TTDSG ist bei einem Teilnehmeranschluss im Haushalt die Mitteilung der Einzelverbindungen nur zulässig, wenn der Anschlussinhaber in Textform erklärt hat, dass er alle zum Haushalt gehörenden Personen darüber informiert hat und künftige Mitnutzer des Teilnehmeranschlusses unverzüglich darüber informieren wird.

Gespräche zu bestimmten sozialen Einrichtungen (§ 11 Abs. 5 TTDSG, z. B. zur Telefonseelsorge) dürfen nicht auf dem Einzelverbindungsnachweis erkennbar sein.

3.3 E-Mail

Mit dem aktuellen TKG ist auch das Angebot eines E-Mail-Dienstes grundsätzlich als Telekommunikationsdienst anzusehen.

3.3.1 Datenschutzrechtliche Pflichten des E-Mail-Providers

Der Anbieter eines E-Mail-Dienstes ist ein Anbieter von Telekommunikationsdiensten im Sinne des TKG und damit zur Einhaltung der Datenschutzgrundsätze des TTDSG und des TKG verpflichtet. Außerdem muss er die notwendigen technischen und organisatorischen Maßnahmen nach § 165 TKG und Art. 32 DSGVO einhalten. Für technische Details bei der Übermittlung und Verarbeitung der Daten, die sich auf den Transport beziehen, ist der E-Mail-Diensteanbieter damit datenschutzrechtlich Verantwortlicher. Die datenschutzrechtliche Zuständigkeit liegt gemäß § 29 TTDSG grundsätzlich beim BfDI.

3.3.2 Datenschutzrechtliche Pflichten für den Anwender von E-Mail-Diensten

Von der Sphäre des E-Mail-Providers ist die Sphäre des Anwenders oder Versenders einer E-Mail zu unterscheiden. Der Anwender ist seinerseits kein Telekommunikationsanbieter und auch nicht für den Übertragungsvorgang datenschutzrechtlich verantwortlich. Er ist aber datenschutzrechtlich verantwortlich für die Daten, die er im Zusammenhang mit dem Versenden der E-Mail verarbeitet.

Praktische Auswirkungen

Der Versender einer E-Mail muss letztlich eine datenschutzrechtliche Risikoabwägung durchführen, ob eine E-Mail in Bezug auf die konkret betroffenen Daten überhaupt das geeignete Medium ist, welche Verschlüsselung er wählen soll und welcher E-Mail-Anbieter dafür in Betracht kommt. Natürliche Personen unterliegen bei persönlichen oder familiären Tätigkeiten zwar grundsätzlich nicht dem Datenschutzrecht. Aber auch hier kann nur empfohlen werden, besonders sensible Daten nicht ungeschützt per E-Mail zu versenden.

3.3.3 Praxisfragen und Datenverarbeitung beim E-Mail-Zugangsdienst

Es gibt mehrere Möglichkeiten, einen E-Mail-Account zu erhalten. Häufig wird zusammen mit einem Internetzugang ein E-Mail-Account zur Verfügung gestellt. Viele Anbieter ermöglichen einen kostenlosen Account, der dann allerdings oftmals mit mehr Werbung einhergeht. Kostenpflichtige E-Mail-Accounts bieten meist ein umfangreiches Leistungsspektrum, z. B. ein höheres Speichervolumen und weniger Werbemails. Bei einem E-Mail-Account, der bei einem Internetzugang enthalten ist, sind die Bestandsdaten dem Anbieter bekannt und erweitern sich nur um die E-Mail-Adresse und das Passwort. Anders als bei vielen kostenfreien Webmailangeboten verfügt der Telekommunikationsanbieter in jedem Fall über die korrekten Bestandsdaten zu dem E-Mail-Account seiner Kundinnen und Kunden, die er für Auskünfte gemäß §§ 172 und 173 TKG speichern muss (siehe Abschnitt 3.13. zu Überwachungsmaßnahmen und Auskünfte für Behörden).

Die E-Mail-Provider erheben teils umfangreiche Bestandsdaten. Auf den ersten Blick erscheint dies zumindest bei den kostenfreien Tarifen nicht erforderlich, wird aber nachvollziehbar mit den Pflichten des Providers begründet, z. B. bei Haftungsfragen und namensrechtlichen Problemen. Die E-Mail-Adresse ist im Rahmen der Verfügbarkeit vom Nutzenden frei wählbar, das heißt es besteht die Möglichkeit, die Nachrichten unter einem Pseudonym zu versenden. Vielfach werden die von den Nutzenden angegebenen Daten aber nicht verifiziert, sondern

nur auf Plausibilität überprüft. Bank- und Kreditkartendaten darf der Anbieter nur dann erheben, wenn Nutzende sich für einen kostenpflichtigen Tarif angemeldet oder vom kostenfreien in einen kostenpflichtigen gewechselt haben.

Kostenfreie Tarife sind meist werbefinanziert. Oftmals wird ein Newsletter versandt, den die Kundin bzw. der Kunde im Freemail-Tarif nicht abbestellen kann und der neben Informationen zu Produktneuheiten auch verschiedene Werbebotschaften enthält. Der Widerspruch gegen die Zusendung eines Newsletters mit eigenen Angeboten des Providers muss jedenfalls bei einem kostenpflichtigen Angebot möglich sein, ebenso ein völlig werbefreier E-Mail-Account. Will der Provider auch fremde Werbung versenden, benötigt er die Einwilligung seiner Kundinnen und Kunden.

E-Mail-Provider sind nicht verpflichtet, Bestandsdaten eigens für Auskunftsersuchen der Sicherheitsbehörden zu erheben und zu speichern, sondern müssen diese Daten nur dann für die genannten Zwecke bereithalten, wenn sie diese sowieso für ihre eigenen Zwecke speichern.

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

Da das Aufkommen unerwünschter Werbemails (Spam) immer mehr zugenommen hat und durch Spam-Mails auch Viren und Trojaner verbreitet und unvorsichtige Nutzer auf Abzockseiten geleitet werden, setzen die E-Mail-Provider sogenannte Spam-Filter und Virenscanner ein. Durch den Einsatz von Blocklists (Listen von Servern, von denen bekanntermaßen Spam-Mails versendet werden) und durch das sogenannte Greylisting, bei den E-Mails von unbekannten Absendern erst nach einem erneuten Melden des absendenden Servers angenommen werden, können viele Spam-Mails abgewiesen werden. Zusätzlich bieten die E-Mail-Provider Spam-Filter für das Postfach des Nutzers an, die selbständig aktiviert und konfiguriert werden können.

Die Virenscanner überprüfen die Inhalte ein- und ausgehender E-Mails auf verdächtigen Schadcode. Dies geschieht automatisiert.

Die Verwendung der Verkehrsdaten und das automatisierte Prüfen der E-Mail-Inhalte auf Schadcode sind in den engen Grenzen von § 3 Abs. 3 und § 12 TTDSG zulässig; der Provider kann sich zum Schutz der technischen Systeme im dafür erforderlichen Maß Kenntnis vom Inhalt und den Umständen der Telekommunikation verschaffen.

3.4 Festnetztelefonie

Die Telefonie von einem stationären Anschluss aus erfolgt heute praktisch nicht mehr über eine klassische Sprachübermittlung (z. B. ISDN-Anschluss), sondern durch die Übermittlung der Sprachinformationen über Daten-Pakete.

3.4.1 Voice over IP

Voice over IP (VoIP), IP-Telefonie oder aber auch Internettelefonie beschreibt die Verwendung von Netzwerken auf Basis des Internet-Protokolls als Transportmedium für Telefongespräche. Dabei wird die Sprache in viele kurze IP-Pakete verpackt. Bei Telefonanlagen werden die Pakete nur in einem lokalen Netzwerk (LAN) verschickt, bei Netzbetreibern, die gleichzeitig den Internet-Zugang zur Verfügung stellen, werden die Pakete über dessen Netze übertragen, bei anderen Telefondienst-Anbietern laufen die Pakete sogar über beliebige Verbindungen im Internet.

Gerade im letzten Fall ist kaum vorhersehbar, welche Wege die IP-Pakete nehmen und somit, ob jemand mithört. Aber auch in den anderen Fällen sind Angriffe nicht ganz auszuschließen. So könnte ein Gerät im LAN kompromittiert sein und versuchen, Telefonate abzuhören. Die für VoIP meist verwendeten Protokolle SIP (Session Initiation Protocol; zur Steuerung) und RTP (Real-Time Transport Protocol) für die Sprachübertragung sind zunächst einmal nicht verschlüsselt. Hier sollte man die verschlüsselten Varianten SRTP (Secure Real-Time Transport Protocol) und SIPS (Session Initiation Protocol) nutzen. Viele Router und viele Telefonanbieter ermöglichen bereits eine verschlüsselte Kommunikation. Manchmal muss man dies im Router noch selbst aktivieren.

3.4.2 Drahtlose Kommunikation für die Telefonie im Festnetz

Im Festnetz werden seit vielen Jahren häufig schnurlose DECT-Telefone verwendet. Um ein Abhören dieser Funk-Übertragung zu verhindern, bietet der DECT-Standard schon lange eine Verschlüsselung an. Diese ist jedoch optional. Außerdem gibt es mehrere Generationen, von denen gerade die ältere 64-Bit-Variante nicht mehr als besonders sicher gelten kann. Auch die Verwendung von Telefon und Basisstation verschiedener Hersteller kann bei der Verschlüsslung problematisch sein. Für den Betrieb von Repeatern kann es erforderlich sein, die Verschlüsselung zu deaktivieren. Damit verzichtet man allerdings auf jeden Abhörschutz.

Insofern ist es empfehlenswert, beim Kauf von DECT-Telefonen auf eine moderne Verschlüsselung zu achten und auch bei vorhandenen Geräten einen Blick in die technischen Daten zu werfen. Leider werden hier oft nur unzureichende Informationen zur Verfügung gestellt.

3.4.3 Telefonanlagen

Moderne Telefonanlagen nutzen ebenfalls die VoIP-Technologie, ggf. auch das selbe Netz wie die übrige Informationstechnik. Wenn früher das Netz ausschließlich zum Telefonieren zur Verfügung stand, so war es nur mit großem technischem Aufwand und mit hohem Zusatzwissen möglich, Daten aus diesem Netz unbefugt abzufangen und zu verwerten, z. B. jemanden zu „belauschen“. Hybride Netze „erleichtern“ den Aufwand erheblich, Daten abzufangen, insbesondere, wenn die Netze keine Zugangsbeschränkung aufweisen. Entweder schafft man Vertraulichkeit im Datenverkehr, indem man eine Verschlüsselung einführt, oder man sichert das gesamte Netz (dann ausschließlich für VolP) gegen Eindringlinge ab – im Idealfall kommt beides kombiniert zum Einsatz.

Bei Telefonanlagen sollte man auch prüfen, wie lange man Verkehrsdaten speichern muss und für welchen Zweck. Nicht mehr erforderliche Daten sind zu löschen. Dabei sind die Vorgaben der DSGVO und – sofern ein Telekommunikationsdienst erbracht wird (siehe Abschnitt 2.1 zu Telekommunikations-Dienstleister) – des TTDSG sowie des TKG zu berücksichtigen. Für die meisten Behörden der Bundesverwaltung ist die Richtlinie Telekommunikation Bund (RLTk Bund) zu beachten

in der auch Vorgaben zur Speicherung der Verkehrsdaten gemacht werden.

Die Richtlinie Telekommunikation Bund finden Sie hier:

(QR-Code scannen oder klicken)

Generell empfiehlt es sich, bereits im Vorfeld der Beschaffung einer TK-Anlage zu prüfen, wann Daten zu löschen sind und ob dies umgesetzt werden kann.

Die Mitarbeitenden oder sonstigen Nutzenden einer TK-Anlage sind entsprechend über die Datenverarbeitung zu informieren, z. B. in einer Dienstvereinbarung oder Datenschutzerklärung.

3.4.4 Virtuelle Telefonanlagen

Als Alternative zu einer selbst betriebenen Telefonanlage kann man diese als Dienstleistung beziehen. Solche virtuellen Telefonanlagen basieren heute fast ausnahmslos auf der VoIP-Technologie. Der TK-Anbieter hält dafür in seinem Rechenzentrum für die jeweiligen Kundinnen und Kunden eine eigene virtuelle Telefonanlage bereit, die über Wartungsschnittstellen (z. B. eine Weboberfläche) selbst konfiguriert und betreut werden können. Der technische Betrieb sowie die Wartung der Technik der Anlage obliegen dem Anbieter. Die Kunden müssen in den Räumlichkeiten lediglich die notwendige Anzahl an Endgeräten sowie einen geeigneten Internetanschluss bereithalten.

In technischer Hinsicht ist bei der Verwendung einer virtuellen Telefonanlage grundsätzlich kritisch zu bewerten, wenn die Anbindung der Telefone an die Anlage unverschlüsselt über das Internet erfolgt. Beim Einsatz einer solchen Anlage kann z. B. ein verschlüsseltes VPN (Virtual Private Network) eingesetzt werden. Eine Verschlüsselung von Inhalten und Signalisierung ist anzustreben. Der Standort des

Rechenzentrums, das den Betrieb der Anlage sichert, sollte vertraglich festgehalten werden, da es unter Umständen rechtliche Implikationen geben kann, wenn es um Daten geht, die innerhalb der TK-Anlage gespeichert werden. Hiervon sind nicht nur die Anruflisten und Einzelverbindungsnachweise (EVN) betroffen, sondern möglicherweise im System gespeicherte Adress- und Telefonbücher.

3.4.5 Telefax

Das Telefax ist zwar technisch überholt, wird aber noch gelegentlich verwendet. Ein Telefax wird über einen Sprach-Kanal übertragen, heute also über eine VoIP-Verbindung. Insofern hängt die Sicherheit von der Vertrauenswürdigkeit der beteiligten Netzbetreiber ab. Hinzu kommt, dass nicht mehr jeder Empfänger ein Fax-Gerät nutzt, sondern häufig ein sogenanntes Fax-to-E-Mail Gateway verwendet wird. In diesem Fall treten die Sicherheitsrisiken der E-Mail-Kommunikation hinzu. Dies ist für den Absender aber nicht erkennbar. Es ist also nicht empfehlenswert, besonders sensible Daten per Telefax zu versenden.

3.5 Gesprächsaufzeichnung

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

Wer eine Gesprächsaufzeichnung unbefugt fertigt, verletzt die Vertraulichkeit des Wortes und begeht eine Straftat, die auf Antrag strafrechtlich verfolgt wird. Eine Gesprächsaufzeichnung ist nur dann zulässig, wenn die Einwilligung des Anrufers über die Tastatur oder über die Sprachsteuerung vor Aufzeichnungsbeginn per Zustimmung des Betroffenen eingeholt wird (sogenanntes Opt-In-Verfahren).

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

Solche Mitschnitte gelten als personenbezogene Daten und unterfallen somit auch dem Auskunftsrecht nach Art. 15 DSGVO sowie dem Recht auf Löschung gemäß Art. 17 DSGVO.

3.6 Internetzugangsdienst

Ein Internetzugangsdienst ist gemäß § 3 Nr. 61 lit. a) TKG ein Telekommunikationsdienst. Der Umfang der Erbringung des Telekommunikationsdienstes und damit die Anwendbarkeit des TKG erstreckt sich nur auf die Einrichtung und Bereitstellung des Internetzugangs als solchen und nicht auf Nutzung des Internetzugangs mit Bezug auf die Inhalte oder die Kommunikation des Endgeräts mit anderen Endgeräten. Bei letzterem handelt es sich typischerweise um Telemedien, die nicht dem TKG und den Telekommunikationsregelungen des TTDSG im zweiten Teil unterfallen.

3.6.1 Internetzugang

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

Wird die Zugangskomponente im Netz angeschlossen, wird der Teilnehmer angemeldet und erhält eine IP-Adresse aus dem Adressbestand. IP-Adressen, sowohl zeitlich stabil vergeben oder dynamisch zugeteilt, sind personenbezogene Daten, anhand derer die Anbieter die jeweiligen Kundinnen und Kunden identifizieren können. Die Zuordnung, welche IP-Adresse ein Nutzer zu einem bestimmten Zeitpunkt erhalten hat, wird in speziellen Logfiles gespeichert. Der BfDI hält es für zulässig, diese Daten für Datensicherheitszwecke bis zu sieben Tage zu speichern. Unter bestimmten Voraussetzungen können Strafverfolgungsbehörden die Herausgabe dieser Daten verlangen, um sie zur Ermittlung von Anschlüssen zu nutzen, soweit dies zur Verfolgung

einer Straftat oder Ordnungswidrigkeit erforderlich ist (siehe Abschnitt 3.13 zu Überwachungsmaßnahmen und Auskünfte für Behörden).

Auch bei vermuteten Urheberrechtsverletzungen wird ggf. auf diese Logfiles zurückgegriffen. Eine Sonderstellung im Bereich des Internetzugangs nehmen die sogenannten URLs (Uniform Resource Locator) ein. Beim Surfen gibt der Nutzer in seinem Browser eine bestimmte URL ein, die von einem DNS-Server (Domain Name System) in eine IP-Adresse umgesetzt wird. Auf diesem Wege wird der richtige Ort im Internet adressiert und der Nutzer erhält die gewünschten Daten. URLs können Hinweise auf die Interessen und Vorlieben des jeweiligen Nutzers geben. Daher sind die URLs als besonders schützenswerte Inhaltsdaten anzusehen und dürfen vom Telekommunikationsanbieter nicht gespeichert werden.

Für Zwecke der Erkennung, Eingrenzung und Beseitigung von Störungen ermöglicht § 12 Abs. 1 TTDSG die Speicherung der Verkehrsdaten sowie von Steuerdaten informationstechnischer Protokolle, jedoch nicht von Inhaltsdaten. Ein Zeitraum von höchstens sieben Tagen wird aufgrund langjähriger Erfahrung zunächst als ausreichend angesehen. Sind konkrete Anhaltspunkte für eine Störung festgestellt worden, dürfen im Einzelfall die zum Eingrenzen und Beseitigen der vermuteten Störung erforderlichen Daten länger gespeichert werden. Darüber hinaus kann mit Statistiken oder anonymisierten Daten gearbeitet werden.

In § 169 Abs. 4 bis 7 TKG werden dem Netzbetreiber Maßnahmen zur Information des Nutzers sowie Umleitung des Verkehrs oder Sperrung des Anschlusses erlaubt, um Störungen zu beseitigen, die von Systemen des Nutzers ausgehen. Dies ist für Fälle gedacht, bei denen ein Gerät (z. B. PC) des Kunden von Schadsoftware betroffen ist und andere Nutzer des Internets stört.

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

nehmer der Kommunikation bleiben für einen potentiellen Angreifer ersichtlich, die Inhalte der Kommunikation sind jedoch verschlüsselt und nicht direkt abgreifbar.

3.6.2 Internetprotokollversionen

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

Der Adressierungsbereich von IPv4 wurde in den Anfängen des Internets festgesetzt. Die knapp über vier Milliarden Adressen reichen schon seit langem nicht mehr aus, alle Geräte anzubinden. Allerdings sind die IPv4-Adressen einfacher aufgebaut als die neuen IPv6-Adressen, so dass noch vielfach die IPv4-Adressen verwendet werden.

Wegen der oftmals nicht ausreichenden Anzahl wird dann ein Pooling-Verfahren angewendet, das sogenannte nating (NAT = Network Address Translation). Dabei wird beim Service Provider einem Kunden nur temporär eine öffentliche IP-Adresse zugeteilt (sogenannte dynamische Adresszuteilung). Die private IP-Adresse des Kunden bleibt dann verborgen. Dies hat den aus Datenschutzsicht positiven Nebeneffekt, dass nicht jeder einzelne Nutzer im Internet direkt anhand der IP-Adresse erkennbar ist. Eine Zuordnung könnte nur durch eine Abfrage der jeweiligen sogenannten Port-Nummer beim Service-Anbieter erfolgen, sofern diese dort aus technischen Gründen überhaupt aufgezeichnet wird.

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

Eine IPv6-Adresse besteht aus zwei gleich großen Teilen, *Präfix* und *Interface Identifier* genannt. Die Länge der IPv6-Adresse bewirkt, dass ein Nutzer grundsätzlich allein anhand des Präfix als auch allein durch den Interface Identifier eindeutig bestimmt werden kann. Deshalb sind für beide Teil-Adressen Vorkehrungen erforderlich, die diesem Identifizierungsrisiko begegnen.

Der vordere Teil, das sogenannte *Präfix*, wird vom Provider bestimmt und dem Anschluss des Nutzers zugewiesen. Hier gibt es ähnlich wie beim „alten" IPv4 unterschiedliche Arten der Zuweisung. Einem Anschluss kann entweder dauerhaft (also statisch) oder wechselnd (also dynamisch) ein Präfix zugeteilt werden. Die meisten Provider haben sich für die dynamische Vergabe entschieden.

Der hintere Teil der Adresse, der sogenannte *Interface Identifier*, wird vom Endgerät des Nutzers bestimmt. Da nicht nur das Präfix datenschutzrechtlich bedeutsam ist, sind auch hier Maßnahmen gefragt, die den Adressbestandteil veränderlich halten. Der Standard zu IPv6 empfiehlt zu diesem Zweck den Einsatz der sogenannten *Privacy Extensions* (Datenschutzerweiterungen). Diese sorgen nicht nur dafür, dass die eindeutige Hardwareadresse der Netzwerkkarte keinen unmittelbaren Eingang in die Adresse findet, sondern bewirken ferner einen regelmäßigen Wechsel der Netzwerkkartenkennung. Die Privacy Extensions sollten entsprechend grundsätzlich aktiviert sein.

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

3.7 Messenger-Dienste

Zu einem großen Teil findet Kommunikation heute über mobile Geräte und entsprechende Apps statt. So werden mit Messenger-Apps nicht nur Textnachrichten oder Sprachaufnahmen verschickt, sondern auch Fotos und Videos geteilt.

Als sogenannte OTT-Dienste unterfallen diese Messenger-Dienste nach der TKG-Novelle ebenfalls den telekommunikationsrechtlichen Regelungen.

Datenschutzrechtlich relevant sind neben dem Schutz des Kommunikationsinhaltes (Stichwort: Profilbildung) und der Bestandsdaten insbesondere die Zugriffsrechte, z. B. auf Kontaktlisten oder Standortda-

ten, die dem Messenger-Dienst eingeräumt werden sowie der Umgang mit den Betroffenenrechten.

Mehr zu Messengerdiensten finden Sie hier:

(QR-Code scannen oder klicken)

3.8 Mobilfunk

Als Geräte für die mobile Kommunikation werden heute Smartphones, klassische Handys, Notebooks oder Tablets mit Mobilfunkschnittstellen, aber auch sogenannte Wearables (z. B. Smartwatch) verwendet. Aus technischer Sicht differenziert man bei der Mobilkommunikation zwischen verschiedenen Standards, wie z. B.

- GSM (Global System for Mobile Communications),
- UMTS (Universal Mobile Telecommunications System),
- LTE (Long Term Evolution) und
- 5G (fünfte Generation).

Diese unterscheiden sich dabei u. a. in den genutzten Frequenzen, der Art der Modulation und der Latenz, wodurch unterschiedliche Datenübertragungsraten und Zellgrößen zur Flächenversorgung resultieren.

3.8.1 GSM

In den Mobilfunknetzen nach dem GSM-Standard (Standard 2. Generation) werden Sprache und Daten digital übertragen. Die digitalen Daten werden für die Übertragung verschlüsselt. Der verwendete kryptographische Algorithmus als auch die Schlüssellänge entsprechen jedoch nicht mehr dem Stand der Technik, so dass ein Mithören eines Gespräches nicht ausgeschlossen werden kann. Eine weitere Angriffsmöglich-

keit besteht durch eine „gefälschte“ Basisstation (einem sogenannten IMSI-Catcher) eines Angreifers, in die sich ein GSM-Endgerät einbucht.

GSM wird heute noch von einfachen Handys, aber auch von Smartphones als „Rückfall-Ebene“ genutzt, sofern modernere Netze nicht zur Verfügung stehen. Anders als beim Nachfolge-Protokoll UMTS (3. Generation) ist zu erwarten, dass die GSM-Netze noch einige Zeit weiter betrieben werden.

3.8.2 LTE

Der vierte Standard ermöglicht die paketbasierte Übermittlung von Telefonaten. VoLTE (Voice „Sprache“ over LTE) gilt noch als sicher, ist jedoch nicht flächendeckend verfügbar. Sofern das Gerät auf GSM zurückgreifen muss, liegen dieselben Sicherheitsrisiken vor. Auch zu LTE gibt es Informationen zu Sicherheitslücken, die darauf hinweisen, dass ein Einbuchen auf gefälschte Basisstationen und Umleitungen auf gefälschte Webseiten möglich ist.

3.8.3 5G

Mit der fünften Mobilfunkgeneration halten weitere datenschutzrechtliche und sicherheitstechnische Verbesserungen Einzug.

Die Teilnehmeridentität (IMSI) soll nunmehr nur noch verschlüsselt übertragen werden. Ebenso soll auch ein Verbindungversuch mit falschen Mobilfunkstationen abgewehrt werden können. Um den berechtigten Behörden weiterhin die gewohnten Maßnahmen, z. B. zur Feststellung der IMSI zu ermöglichen, werden die Netzbetreiber zur Mitwirkung bei technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten verpflichtet.

Um die Anforderungen an 5G erfüllen zu können, ist eine Erweiterung des bisherigen Mobilfunknetzes notwendig. Mit 5G werden die Frequenzen im Spektrum erweitert, daher müssen vor allem für den hochfrequenten Bereich zusätzliche Access Points aufgestellt werden. Physikalisch bedingt geht mit höheren Frequenzen eine geringere Wellenausbreitung einher und die Funkzelle verkleinert sich. Als Nebeneffekt ist aus Datenschutzsicht zu beachten, dass bei einer Flächenabdeckung durch mehrere kleinere Funkzellen der Standort eines Gerätes noch genauer bestimmt werden kann.

3.9 Notrufe und öffentliche Warnungen/ Cell-Broadcast

Werden Notrufnummern gewählt, sind oft Leben oder Gesundheit von Menschen in Gefahr. Deshalb wird bei Notrufen – anders als bei sonstigen Verbindungen – stets die Rufnummer und der Standort des Anrufers übermittelt (§ 164 TKG). Dies betrifft sowohl den Mobilfunk, bei dem Informationen zur Funkzelle übermittelt werden, als auch die Adresse eines Telefonanschlusses im Festnetz. Diese Daten werden vom Diensteanbieter an die Rettungsleitstelle übermittelt. Die Einzelheiten regeln die Verordnung über Notrufverbindungen und die Technische Richtlinie Notruf. Bei vielen Smartphones kann zusätzlich noch ein vom Gerät (z. B. per Satellitenortung) ermittelter Standort an die Rettungsleitstelle übermittelt werden.

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

Um die Warnung der Bevölkerung bei Notfällen oder Katastrophen zu verbessern, wird mit § 164a TKG die Möglichkeit von öffentlichen Warnungen eingeführt. Mittels sogenannten Cell-Broadcast werden in den Mobilfunk-Netzen Nachrichten versendet, die – ähnlich wie bei einem Rundfunk-Signal – alle Handys empfangen können. Hier ist es ggf. möglich, die Anzeige von Warnungen (mit niedrigeren Warnstufen) am Handy zu deaktivieren.

3.10 Ortung und Standortdaten

Bei dem Betrieb von Mobilfunknetzen werden auch Standortdaten als Teil der Verkehrsdaten verarbeitet. Das Mobilfunknetz muss schließlich wissen, in welcher Funkzelle sich ein Endgerät befindet. Diese Standortdaten werden auch für – wenn auch nur noch wenige – standortabhängige Tarife verarbeitet. Auch um Notrufe der richtigen Rettungsleitstelle zuzuordnen und um dieser den ungefähren Standort mitzuteilen, werden die Standortdaten genutzt. Ebenso sind diese Daten für die Erkennung von Störungen erforderlich.

Regelungen zu Standortdaten

§ 13 TTDSG regelt die Verarbeitung von Standortdaten zur Bereitstellung von Diensten mit Zusatznutzen. Darin wird etwa geregelt, dass eine gesonderte schriftliche Einwilligung und bei jeder Ortung eine Informations-SMS erforderlich ist, wenn Dritte die Standortdaten erhalten. Es gelten also sehr restriktive Anforderungen für die Telekommunikationsanbieter.
Ebenfalls restriktiv sind die Regelungen des § 100i StPO, wonach Ermittlungsbehörden den Standort eines Mobiltelefons abfragen können.

Praktisch wesentlich weitreichendere Auswirkungen für den Datenschutz hat eine Standortbestimmung direkt über das Endgerät über Satelliten-Navigationsdienste wie GPS und WLAN-Kennungen, die durch zahlreiche Apps stattfindet. Diese Standortdaten sind auch wesentlich genauer. Für diese Art der Verarbeitung von Standortdaten greift die Sonderregelung des § 13 TTDSG nicht. Zwar handelt es sich bei § 13 TTDSG um eine Spezialregelung für Standortdaten. Der Anwendungsbereich von § 13 TTDSG, beschränkt sich aber wegen der grundsätzlichen Stellung des § 13 TTDSG in Teil 2 des TTDSG (Datenschutz und Schutz der Privatsphäre in der Telekommunikation) nur auf die Verarbeitung von Standortdaten durch Telekommunikationsdienstleister und ist auch vom Regelungszweck her nicht ohne Weiteres übertragbar. Für die Verarbeitung von Standortdaten, die von den Geräten ermittelt werden gelten daher die allgemeinen Regelungen der DSGVO.

3.11 Rufnummernunterdrückung

Nach § 15 Abs. 1 TTDSG müssen Anrufende und Angerufene die Möglichkeit haben, die vom Diensteanbieter angezeigte Rufnummer des Anrufenden dauerhaft oder für jeden Anruf einzeln auf einfache Weise und unentgeltlich zu unterdrücken. Die Verpflichtung aus § 120 Abs. 1 TKG zur netzseitigen Signalisierung bleibt auch im Falle der Rufnummernunterdrückung nach § 15 Abs. 1 TTDSG unberührt, so dass diese sowohl für Sicherheitsbehörden erkennbar bleibt und auch im Rahmen der Abrechnung zwischen den an der Verbindung beteiligten Netzbetreibern verwendet werden kann. Allein gegenüber dem

Angerufenen wird die Anzeige der signalisierten Rufnummer unterdrückt. Das Recht, die Rufnummernanzeige nach § 15 Abs. 1 TTDSG zu unterdrücken, ist allerdings ausweislich der Regelung in § 15 Abs. 2 TTDSG für Werbeanrufe ausdrücklich ausgeschlossen.

3.12 Teilnehmerverzeichnisse

Auf den Wunsch der Kundin oder des Kunden übermittelt der Telekommunikationsanbieter Name, Anschrift und Rufnummer an die Herausgeber von Telefonverzeichnissen und/oder Betreiber von Auskunfts- bzw. Vermittlungsdiensten zur Aufnahme in die dortigen Telefonverzeichnisse (§ 17 TTDSG). Dabei kann die Kundin oder der Kunde bestimmen, dass die Eintragung nur in gedruckte oder elektronische Verzeichnisse erfolgt. Mitnutzende können eingetragen werden, wenn sie ihr Einverständnis erklärt haben. Auskunftsersuchende, denen nur die Rufnummer der Kundin bzw. des Kunden bekannt ist, erhalten im Rahmen der sogenannten Inverssuche Auskunft über die ggf. veröffentlichten Bestandsdaten.

3.13 Überwachungsmaßnahmen und Auskünfte für Behörden, z. B. bei Strafverfolgung

3.13.1 Allgemeines

Daten, die Telekommunikationsanbieter verarbeiten, sind an vielen Stellen für staatliche Ermittlungsbehörden von Interesse, wenn z. B. eine Telefonnummer oder eine IP-Adresse einer Person zugeordnet werden soll. Zur Verfolgung von schweren Straftaten kommt sogar eine Telefonüberwachung in Betracht. Da es sich hierbei um schwerwiegende Eingriffe in den Privatbereich der Betroffenen handelt, sind dafür normenklar formulierte gesetzliche Ermächtigungsgrundlagen erforderlich.

3.13.2 Doppeltürenmodell

Rechtlich ist im Sinne des Doppeltürenmodells sowohl eine Ermächtigungsgrundlage für das Auskunftsersuchen als auch für die Auskunftserteilung erforderlich. Die Regelungen des TKG zur Auskunftserteilung stellen also keine Rechtsgrundlage für das Auskunftsersuchen dar,

wie das BVerfG in seinem Beschluss vom 24. Januar 2012 ausdrücklich klargestellt hat. Ermächtigungsgrundlagen für Auskunftsersuchen sind in verschiedenen Bundes- und Landesgesetzen geregelt, u. a.

- im Gesetz zu Art. 10 GG,
- in der StPO,
- im Außenwirtschaftsgesetz (AWG) und
- in Landespolizeigesetzen zur Gefahrenabwehr.

Im Folgenden sollen zunächst die Verpflichtungen von Seiten des Telekommunikationsanbieters betrachtet werden und danach die Rechtsgrundlagen für die Behörden, weil auf diese Weise besser verständlich wird, welche Daten überhaupt vorliegen und verwendet werden können. Wegen der grundsätzlichen Ausdehnung des TKG auf weitere Dienste ist mit der TKG-Novelle auch der Umfang der Überwachung in bestimmten Konstellationen gestiegen. Einzelheiten finden sich im 30. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit für das Jahr 2021 des BfDI unter Textziffer 5.1.

Zum 30. Tätigkeitsbericht geht's hier:

(QR-Code scannen oder klicken)

3.13.3 Prüfpflichten der Telekommunikationsanbieter

§ 174 Abs. 2 S. 5 TKG stellt klar, dass die Prüfung der materiellen Zulässigkeit eines Auskunftsersuchens ausschließlich unter die Verantwortlichkeit der abfragenden Stelle fällt. Die Diensteanbieter müssen lediglich das Vorliegen formeller Voraussetzungen (Textformerfordernis, ausdrückliche Benennung der Rechtsgrundlage für die Abfrage, ggf. richterliche Anordnung usw.) kontrollieren. Nur wenn diese

vorliegen, darf dem Ersuchen entsprochen und die begehrte Auskunft erteilt werden.

3.13.4 Regelungen im Telekommunikationsrecht

Im TKG und der TKÜV werden die technischen und verfahrensrechtlichen Einzelheiten verschiedener Methoden und Abfragemöglichkeiten geregelt. Zu unterscheiden ist hier zwischen Überwachungsmaßnahmen und der Erteilung von Auskünften. Für die Auskünfte wiederum ist sowohl ein automatisiertes Auskunftsverfahren für bestimmte Bestandsdaten vorgesehen (§ 173 TKG), als auch ein manuelles Auskunftsverfahren gemäß § 174 TKG für Bestandsdaten.

Nach § 170 TKG gibt es eine gesetzliche Verpflichtung für die Betreiber von Telekommunikationsanlagen, auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung und zur Beantwortung von Auskünften vorzuhalten.

Die Anbieter sind gemäß § 172 TKG verpflichtet, die Bestandsdaten vorsorglich für Zwecke der Strafverfolgung zu speichern.

Derzeit nicht angewendet wird § 176 TKG, der die Pflicht zur Speicherung auch der Verkehrsdaten festschreibt. Dies ist die sogenannte Vorratsdatenspeicherung, die vom Europäischen Gerichtshof als EU-rechtswidrig eingestuft wurde (EuGH vom 20. September 2022, Rechtssachen C-793/19 und C-794/19, SpaceNet AG und Telekom Deutschland GmbH).

3.13.5 Datenerhebung nach § 172 TKG

Konkret sind gemäß § 172 Abs. 1 TKG die folgenden Daten zu erheben:

- Rufnummern und andere Anschlusskennungen,
- Name und Anschrift der/des Anschlussinhaberin/s,
- bei natürlichen Personen deren Geburtsdatum,
- bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
- bei Mobilfunkanschlüssen, bei denen auch ein mobiles Endgerät überlassen wird, die Gerätenummer dieses Gerätes,
- das Datum der Vergabe der Rufnummer und, soweit abweichend, des Vertragsbeginns und

- sobald bekannt, die Beendigung der Zuordnung der Rufnummer und, soweit abweichend, das Datum des Vertragsendes.

Die Diensteanbieter haben darauf zu achten, dass die Daten korrekt und aktuell sind.

Die Kundendateien sind so verfügbar zu halten, dass die BNetzA einzelne Daten oder Datensätze in einem von ihr vorgegebenen automatisierten Verfahren abrufen kann.

Bedarfsträger, die Auskünfte aus den Kundendateien erhalten können, sind nach § 173 Abs. 4 TKG u. a.

- Gerichte und Strafverfolgungsbehörden,
- Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,
- Zollkriminalamt (ZKA) und Zollfahndungsämter (ZFÄ) für Zwecke eines Strafverfahrens sowie das ZKA zur Vorbereitung und Durchführung von Maßnahmen nach § 72 des Zollfahndungsdienstgesetzes (ZfdG),
- Verfassungsschutzbehörden des Bundes und der Länder, Militärischer Abschirmdienst (MAD), Bundesnachrichtendienst (BND),
- Notrufabfragestellen nach § 164 TKG sowie die Abfragestelle für die Rufnummer 124 124,
- die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sowie
- Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes (SchwarzArbG) genannten Zwecke über zentrale Abfragestellen.

3.13.6 Vorab bezahlte Mobilfunkdienste

Nach § 172 Abs. 2 TKG haben die Anbieter von im Voraus bezahlten Mobilfunkdiensten (Prepaid-SIM-Karten) vor der Freischaltung die Richtigkeit der erhobenen Daten anhand eines Ausweisdokuments zu überprüfen. Diese Verpflichtung besteht seit dem 1. Juli 2017 und geht auf Maßnahmen der Bundesregierung im Rahmen der sogenannten Anti-Terror-Gesetzgebung zurück. Die BNetzA hat in diesem Zusammenhang eine Verfügung erlassen, wie diese Überprüfung im

Einzelfall erfolgen muss. Die Telekommunikationsanbieter müssen bei im Voraus bezahlten Mobilfunkdiensten zudem Informationen zum verwendeten Überprüfungsverfahren sowie der Art, Nummer und ausstellenden Stelle des vorgelegten Legitimationsdokuments speichern.

3.13.7 Automatisiertes Abrufverfahren nach § 173 TKG

§ 173 TKG erlaubt eine komplexe Abfrage nach unvollständigen Daten, etwa, wenn nur Teile des Namens oder nicht die genaue Schreibweise (z. B. Maier oder Meyer) bekannt sind. Auch werden weitere Daten übermittelt, etwa das Geburtsdatum oder die zum Anschluss gehörende E-Mail-Adresse. Dies wird in der KDAV und der TR AAV geregelt.

Die BNetzA gibt die abgerufenen Daten an die ersuchende Stelle weiter und protokolliert gemäß § 173 Abs. 8 TKG den Zeitpunkt des Abrufs, die für den Abruf verwendeten Daten, die abgerufenen Daten, die die Daten abrufende Person sowie die ersuchende Stelle und deren Aktenzeichen. Die Protokollierung soll eine umfassende Datenschutzkontrolle ermöglichen.

Datenschutzaufsicht

Ruft die BNetzA Daten für die Polizei eines Bundeslandes ab, kann die zuständige Landesdatenschutzaufsichtsbehörde bei der Polizei kontrollieren, ob die Abfrage zulässig war. Die BNetzA wiederum wird vom BfDI hinsichtlich der datenschutzrechtlichen Verpflichtungen kontrolliert.

Im Gegensatz zu dem Verfahren nach § 174 TKG dürfen die Anbieter für Abfragen nach § 173 Abs. 9 S. 3 TKG den Bedarfsträgern und der BNetzA keine Kosten in Rechnung stellen.

3.13.8 Manuelles Auskunftsverfahren nach § 174 TKG

Neben dem automatisierten Auskunftsverfahren sind die Diensteanbieter auch verpflichtet, manuelle Auskunftsersuchen von Sicherheitsbehörden zu beantworten. Die Auskunftspflicht bezieht sich dabei auf die von diesen erhobenen Bestandsdaten sowie die nach § 172 TKG erhobenen Daten.

IP-Adressen

§ 174 Abs. 1 S. 3 TKG stellt ausdrücklich klar, dass die Auskunftspflicht auch Informationen zum Inhaber eines Anschlusses umfasst, dem zu einem bestimmten Zeitpunkt eine dynamische (öffentliche) Internet-Protocol (IP)-Adresse zugeordnet war.

Diese sogenannte IP-Auskunft bleibt den in § 174 Abs. 3 TKG benannten Stellen vorbehalten.

3.13.9 Vorratsdatenspeicherung nach § 176 TKG

Verkehrsdaten müssen (zumindest derzeit) nicht vorsorglich gespeichert werden (sogenannte Vorratsdatenspeicherung), sondern müssen erst nach Vorliegen einer strafprozessualen Anordnung herausgegeben werden.

§ 176 TKG enthält praktisch inhaltsgleich zu der Vorgängerregelung des § 113b TKG a. F. eine Verpflichtung der Anbieter von Telekommunikationsdiensten, die Verbindungsdaten auf Vorrat für einen Zeitraum von zehn Wochen für Polizei- und Strafverfolgungsbehörden bereitzuhalten. Bei Mobilfunkanschlüssen sind Standortdaten nach Abs. 4 der Norm für vier Wochen zu speichern. Betroffen sind also die Daten „wer mit wem", „wann" und „wo" kommuniziert hat.

Die Regelung wird derzeit durch die BNetzA nicht angewendet. Das Bundesverwaltungsgericht hat die Vorschrift inzwischen mit Urteil vom 14. August 2023 (Az. 6 C 6.22) als Reaktion auf das Urteil des EuGH vom 20. September (siehe unten) als nicht anwendbar erklärt.

Position des BfDI

Aus datenschutzrechtlicher Sicht ist eine Vorratsdatenspeicherung klar abzulehnen. Sie stellt einen massiven Eingriff in die Grundrechte und die Freiheitsrechte vollkommen unbeteiligter Personen dar, deren Daten vom Prinzip her ohne besonderen Anlass „auf Vorrat" gespeichert werden. Dies ist zudem nicht erforderlich, da eine Herausgabe der Daten auf einen konkreten Verdacht hin zulässig ist, so dass es in der Praxis wirksame Instrumente wie etwa das „Quick Freeze-Verfahren" und die „Login-Falle" gäbe.

Der EuGH hat in seinem Urteil vom 20. September 2022 (Rechtssachen C-793/19 und C-794/19 SpaceNet AG und Telekom Deutschland GmbH) die deutschen Vorschriften zur Vorratsdatenspeicherung als nicht mit dem EU-Recht vereinbar erklärt. Im Zuge einer gesetzlichen Neuregelung wird derzeit eine Aufhebung der Regelungen zur Vorratsdatenspeicherung sowie eine Neuregelung für ein „Quick-Freeze"-Verfahren diskutiert.

3.13.10 Telefonüberwachung und Auskünfte an Strafverfolgungsbehörden

Die Ermächtigungsgrundlagen für weitreichende Eingriffe z. B. in das Fernmeldegeheimnis finden sich in der StPO.

3.13.10.1 § 100a StPO (Quellen-TKÜ)

Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I 2017 Seite 3202) wurde in § 100a StPO in Ergänzung zur klassischen TKÜ die Quellen-TKÜ als zusätzliche Maßnahme der Echtzeitüberwachung von Telekommunikationsvorgängen eingeführt. Diese dient der Überwachung verschlüsselter Kommunikation, indem die Daten nicht beim Telekommunikationsanbieter, sondern beim Betroffenen erhoben werden, wo sie unverschlüsselt vorliegen. Diese neu eingeführte Regelung führt nach Auffassung des BfDI zu erheblichen datenschutzrechtlichen Risiken und wird als verfassungsrechtlich problematisch erachtet.

3.13.10.2 Auskunftsersuchen nach § 100g StPO

Nach § 100g Abs. 1 S. 1 StPO dürfen zur Verfolgung bestimmter Straftaten von auch im Einzelfall erheblicher Bedeutung oder wenn eine Straftat mittels Telekommunikation begangen wird, Verkehrsdaten (u. a. nach § 9 Abs. 1 TTDSG) erhoben werden. Diese Daten müssen für die Erforschung des Sachverhaltes erforderlich sein. Die Erhebung der Daten muss ferner in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. Wurde eine Straftat mittels Telekommunikation begangen, ist diese Maßnahme nur zulässig, wenn die Erforschung des Sachverhaltes auf andere Weise aussichtslos wäre. Die Erhebung von Standortdaten ist nur in den engen Grenzen des § 100g Abs. 1 S. 3 und 4 StPO zulässig. Das Auskunftsersuchen ist nach § 101a StPO grundsätz-

lich an das Vorliegen einer richterlichen Anordnung gebunden. Die Vorschrift des § 100g StPO ist eine der in § 9 Abs. 1 S. 4 TTDSG erwähnten „anderen Rechtsvorschriften“ und begründet eine Auskunftspflicht des Diensteanbieters (siehe Kapitel 2.7.5. Verkehrsdaten).

Die in § 100g Abs. 2 StPO vorgesehene Abfrage, von rückwirkend ohne konkreten Verdacht gespeicherten Daten nach § 176 TKG, (Vorratsdatenspeicherung) ist nach dem Urteil des EuGH vom 20. September 2022 (Rechtssachen C-793/19 und C-794/19 SpaceNet AG und Telekom Deutschland GmbH) nicht mit EU-Recht vereinbar. Da aber ohnehin die Speicherung nach § 176 TKG nicht stattfindet (siehe Kapitel 3.13.9. Vorratsdatenspeicherung nach § 176 TKG), gibt es derzeit keine Daten, auf die dort zugegriffen werden könnte.

3.13.10.3 Auskunftsersuchen nach § 100j StPO

§ 100j StPO ermächtigt Strafverfolgungsbehörden, die nach § 172 TKG gespeicherten Bestandsdaten (wie z. B. Name und Anschrift des Anschlussinhabers, zugeteilte Rufnummern und andere Anschlusskennungen) bei Diensteanbietern abzufragen, soweit dies für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Hierunter fallen auch die in § 174 Abs. 1 S. 2 TKG ausdrücklich hervorgehobenen Zugangssicherungscodes, also Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden.

Bei Zugangssicherungscodes schränkt das Gesetz die Abfragemöglichkeit zudem dahingehend ein, dass bereits vor der Abfrage die Voraussetzungen für die spätere Nutzung der Daten vorliegen müssen. Darüber hinaus ist nach § 100j Abs. 3 StPO grundsätzlich eine richterliche Anordnung erforderlich. Schließlich ist in Abs. 4 der Norm eine Benachrichtigungspflicht der von der Auskunft betroffenen Personen vorgesehen, sofern es sich bei dem Auskunftsbegehren um Zugangssicherungscodes oder die Zuordnung von IP-Adressen gehandelt hat.

3.14 Videokonferenz

Mit dem aktuellen TKG sind grundsätzlich auch Videokonferenzen als Telekommunikationsdienst anzusehen. Im TKG vom 1. Dezember 2021 wurde der Begriff der Telekommunikation weit gefasst und umfasst in einem funktionellen Sinn nunmehr alle gewöhnlichen Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglichen (siehe im Einzelnen Definition nach § 3 Nr. 24 TKG). Darunter fallen also auch E-Mails, Voice-Over-IP und Videokonferenzen (sogenannte Over-the-top [OTT]-Anwendungen).

3.14.1 Das Erbringen eines Videokonferenzdienstes im Sinne des TKG und datenschutzrechtliche Verantwortlichkeit

Insbesondere der kommerzielle Anbieter eines Videokonferenzsystems ist ein Anbieter von Telekommunikationsdiensten im Sinne des TKG und damit zur Einhaltung der Datenschutzgrundsätze des TTDSG und des TKG verpflichtet. Außerdem muss er die notwendigen technischen und organisatorischen Maßnahmen nach § 165 TKG und Art. 32 DSGVO einhalten. Der kommerzielle Anbieter des Videokonferenzsystems ist im Zusammenhang mit der Erbringung des Dienstes Videokonferenz als datenschutzrechtlich verantwortliche Stelle zu qualifizieren.

Der Diensterbringer muss daher für die Erbringung des Videokonferenzdienstes die datenschutzrechtlichen Erfordernisse nach der DSGVO beachten. Dazu zählt bspw., dass der Anbieter des Videokonferenzsystems die personenbezogenen Daten, die im Rahmen der Durchführung der Videokonferenz erhoben werden, nur für eigene Zwecke verarbeitet, wenn es hierfür eine Rechtsgrundlage gibt. Bei der Übermittlung ins Drittland sind die Vorschriften der Art. 44 ff. DSGVO zu beachten.

Weiterführende Informationen zu Videokonferenzdiensten finden Sie hier:

(QR-Code scannen oder klicken)

Datenschutzaufsicht

Die datenschutzrechtliche Zuständigkeit für kommerzielle Anbieter von Videokonferenzsystemen liegt gemäß §§ 1 Abs. 3, 29 TTDSG und 9 Abs. 1 BDSG beim BfDI.

3.14.2 Datenschutzrechtliche Pflichten für Anwender von Videokonferenzdiensten

Welche Inhalte und personenbezogenen Daten Gegenstand einer Videokommunikation sind, wird von den jeweiligen Anwendern des Systems bestimmt. Betroffene Daten können hier sowohl Namen und ggf. E-Mail-Adressen der eingeladenen Teilnehmerinnen und Teilnehmer sein, als auch Inhalte, die in der Videokonferenz besprochen werden, sofern es sich um personenbezogene Daten handelt. Mit Blick auf diese personenbezogenen Daten ist der Anwender des Systems datenschutzrechtlich verantwortlich.

Dem Unternehmen oder der Behörde obliegt die Risikoabwägung, ob eine Videokonferenz überhaupt stattfindet, welches Videokonferenzsystem verwendet wird (z. B. eigenes oder externes System) und welche besonderen Einstellungen die Sicherheit der personenbezogenen Daten zusätzlich gewährleisten können.

Für die Abwägung ist das Gesamtgefährdungspotential der konkret betroffenen personenbezogenen Daten von besonderer Bedeutung. Hier gibt es verschiedene Parameter. So ist ein besonders hohes Gefähr-

dungspotential zu sehen, wenn besonders sensible Daten nach Art. 9 DSGVO betroffen sind oder wenn die Teilnehmerinnen und Teilnehmer einer Videokonferenz im Rahmen eines grundsätzlich bestehenden Abhängigkeitsverhältnisses an dieser teilnehmen, wie etwa in der Schule oder auch im Arbeitsverhältnis.

3.15 Wireless LAN (WLAN)

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

Diese Freiheit wird durch Funktechnik ermöglicht. Die Informationen werden zwischen den Endgeräten und dem sogenannten Access Point über die Luft übertragen. Was einen großen Komfort in der Nutzung gewährleistet, birgt jedoch auch Gefahren. Ist ein Gebäude mit der Funkinfrastruktur abgedeckt, so ist damit auch immer außerhalb des Gebäudes ein Empfang der Funkwellen möglich. Mitschnitte und Manipulationen der übertragenen Daten sind so möglich, wenn keine Schutzmaßnahmen eingeführt werden. Eine Verschlüsselung der Verbindung ist daher essentiell. Zur Verschlüsselung stellen die meisten Geräte verschiedene Verfahren zur Verfügung. Von den gängig angebotenen Verfahren kann erst das WPA2-Verfahren (Wi-Fi Protected Access) als recht sicher angesehen werden. Sofern schon verfügbar sollte besser noch die neue Version WPA3 genutzt werden. Wird der Access Point selbst betrieben, kann zudem ggf. die Veröffentlichung des Netzwerknamens (SSID) unterdrückt werden. Aus datenschutzrechtlicher Sicht ist auch ratsam, wenn der Netzwerkname selbst keinen direkten Personenbezug zum Betreiber ermöglicht.

Öffentliche WLAN-Hot-Spots, wie z. B. an Flughäfen oder Bahnhöfen, nehmen unter den Drahtlosnetzwerken einen Sonderstatus ein. Hot-Spots verfügen oft nicht über ein Verschlüsselungsverfahren als Schutz gegen unbefugten Zugang oder Abhören und bieten somit jedem den Zugriff auf das drahtlose Netzwerk mit allen darin vorhandenen Daten. Sogenannte Man-in-the-middle-Attacken, bei denen durch geschickte Positionierung von Funkkomponenten echte Gegen-

stellen vorgegaukelt werden, und die z. B. die Datenübertragung zu bestimmten Netz-Segmenten protokollieren oder blockieren können, sind denkbar. Die Verwendung eines verschlüsselten Kanals (VPN) für alle Anwendungen bzw. einzelner verschlüsselter Verbindungen (https, SSL/TLS) sollte deswegen in dieser Konstellation obligatorisch sein.

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

WLAN wird auch von einigen Unternehmen zur Standortbestimmung genutzt. Über diese Standortbestimmungen können Bewegungsprofile erstellt werden.

Zugrunde liegende Gesetze

Scannen oder klicken Sie auf den jeweiligen QR-Code.
So gelangen Sie zum entsprechenden Gesetz bzw. zur Verordnung, auf die Bezug genommen wird.

Telekommunikationsgesetz (TKG)

Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Datenschutz-Grundverordnung (DSGVO)

Bundesdatenschutzgesetz (BDSG)

ePrivacy-RL
Konsolidierte Fassung ohne EG

ePrivacy-RL
Ursprüngliche Fassung mit EG

Europäischer Kodex für die elektronische Kommunikation

Grundgesetz (GG)

Telemediengesetz (TMG)

Strafgesetzbuch (StGB)

Strafprozessordnung (StPO)

Telekommunikationsüberwachungs verordnung(TKÜV)

Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunfts-ersuchen für Verkehrsdaten (TR TKÜV)

Kundendatenauskunftsverordnung (KDAV)

Technische Richtlinie Automatisiertes Auskunftsverfahren (TR-AAV)

Verordnung über Notrufverbindungen (NotrufV)

Technische Richtlinie Notrufverbindungen (TR Notruf)

www.bfdi.bund.de