Deutscher Bundestag
19. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 19(9)1044
20. April 2021

bitkom

Auf einen Blick

TTDSG

Ausgangslage

Das BMWi hat im Januar 2021 den Referentenentwurf des TTDSG vorgelegt, das insbesondere Rechtsunsicherheiten durch das Nebeneinander von Regelungen der DS-GVO, TMG und TKG adressieren soll. Das Bundeskabinett hat den Entwurf am 10. Februar beschlossen.

Bitkom-Bewertung

Geht in die richtige Richtung: Wir begrüßen, dass der Entwurf bestehende Rechtsunsicherheiten durch die verschiedenen Datenschutzregelungen (u.a. im TK-Bereich) adressiert. **Unser Ziel ist** ein kohärenter Regulierungsrahmen, der die europäischen Entwicklungen einbezieht und Rechtssicherheit für Anbieter und Nutzer schafft.

Das Wichtigste

Im Bitkom sind neue Anbieter genauso wie Mitglieder mit großer Nähe zu den klassischen Diensten vertreten. Unser Papier zeichnet daher mögliche Kompromisslinien vor:

- **Rechtssicherheit**
  Der Entwurf wirft an vielen Stellen vor allem definitorische Fragen auf und klärt die Verhältnisse zu bestehenden oder in Arbeit befindlichen regulatorischen Neuerungen nicht abschließend. Klarstellungen sind daher notwendig.
- **Anwendungsbereich**
  Der Anwendungsbereich des Entwurfs scheint an mehreren Stellen (Alltags-)Geräte zu erfassen und neuen Regelungen oder sogar Verboten zu unterwerfen. Hier bedürfen insbesondere die Regelungen des § 8 und des § 22 der Nachbesserung.
- **Aufsicht**
  Neue aufsichtsrechtliche Zuständigkeiten könnten zu einer Verbesserung im Sinne einer Harmonisierung von aufsichtsbehördlicher Interpretation von Datenschutzvorschriften beitragen. Der hier vorgelegte Vorschlag geht jedoch fehl und bedarf der Klärung.

Bitkom-Zahl

79 Prozent
Acht von zehn Unternehmen sehen in Datenschutzanforderungen die größte Hürde beim Einsatz neuer Technologien (lt. einer Studie von Bitkom Research).

Stellungnahme

TTDSG

April 2021

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Nick Kriegeskotte
Leiter Infrastruktur & Regulierung
T +49 30 27576 224
n.kriegeskotte@bitkom.org

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Einleitung

Am 12. Januar 2021 legte das Bundesministerium für Wirtschaft und Energie (BMWi) den Referentenentwurf für das Telekommunikations-Telemedien-Datenschutzgesetz (im Folgenden: TTDSG) vor (die Bitkom Kommentierung des Referentenentwurfs ist hier abrufbar). Das Bundeskabinett hat den Entwurf am 10. Februar beschlossen. Das TTDSG soll vor allem bestehende Rechtsunsicherheiten beheben, die durch das Nebeneinander der den Datenschutz betreffenden Regelungen aus DS-GVO, TMG und TKG entstanden sind. Gegenüber dem im Sommer 2020 bekannt gewordenen Entwurf des TTDSG stellen wir bereits einige wichtige Veränderungen und Klarstellungen fest. Ein funktionierender Datenschutzrahmen muss zwingend aus einem kohärenten Regelungssystem bestehen, ohne Doppelregulierung oder sich widersprechender Pflichten und Zuständigkeiten. Nur so kann durch den Rechtsrahmen die erfolgreiche Entwicklung der Datenökonomie und ein funktionierender Datenschutzrahmen für die Betroffenen vorangetrieben werden. Es ist daher richtig und wichtig, dass der Gesetzentwurf die Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 sowie des Kodex für die elektronische Kommunikation (EKEK), die TKG-Novelle beachtet und in ein inhaltlich stimmiges Rahmenwerk zusammenführen will. Aus unserer Sicht ist es daneben zwingend erforderlich auch die Entwicklungen hinsichtlich des Data Governance Acts und der ePrivacy Verordnung auf europäischer Ebene zu berücksichtigen.

Detailkommentierung zum Regierungsentwurf des TTDSG

a. § 1 Anwendungsbereich des Gesetzes

Der in § 1 geregelte Anwendungsbereich bedarf der Nachschärfung. So bestimmt bereits § 1 Abs. 1 den Anwendungsbereich und nimmt in Nr. 1 das Fernmeldegeheimnis in den Anwendungsbereich auf. Unklar ist hingegen die Regelung des § 1 Abs. 2, der in den

Regelungen zu Anwendungsbereich des Gesetzes den Inhalt des Fernmeldegeheimnisses für juristische Personen festlegt. Eine solche Regelung sollte nicht in den Bestimmungen zum Anwendungsbereich, sondern allenfalls in den Bestimmungen zum Fernmeldegeheimnis in § 3 Ref-E geregelt sein.

Auch ist der Regelungsinhalt von § 1 Abs. 2 unklar. Die Norm trifft keine klare Aussage darüber, ob bestimmte Einzelangaben von juristischen Personen dem Fernmeldegeheimnis unterliegen, sondern versucht eine Gleichstellung zu den personenbezogenen Daten. Das Fernmeldegeheimnis dient aber nicht dem Schutz personenbezogener Daten, sondern der Vertraulichkeit der Telekommunikation.

Zudem bedarf es einer Regelung des Inhalts des § 1 Abs. 2 nicht. Es sollte nur die Telekommunikation natürlicher Personen dem Fernmeldegeheimnis unterliegen. Handeln natürliche Personen für Juristische, unterliegt auch diese Kommunikation dem Fernmeldegeheimnis, da sie von natürlichen Personen geführt wird. Eine Erweiterung des Fernmeldegeheimnisses auf die Telekommunikation juristischer Personen sollte daher unterbleiben. Vielmehr ist die Ausdehnung des Fernmeldegeheimnisses auf die Kommunikation juristischer Personen für Industrievernetzung und M2M Anwendungen kontraproduktiv. Diese Kommunikation sollte gerade nicht dem Fernmeldegeheimnis unterliegen, um Zugriff auf diese Kommunikation für Anwender zu ermöglichen.

In § 1 Abs. 3 wird der territoriale Anwendungsbereich des TTDSG festgelegt. Danach findet es Anwendung auf Unternehmen, die in Deutschland eine Niederlassung haben oder in Deutschland Dienstleistungen erbringen oder hieran mitwirken. Nach der Begründung soll hierdurch das Marktortprinzip festgelegt werden. Man scheint sich diesbezüglich an der DSGVO orientieren zu wollen, ohne jedoch entsprechend flankierende Mechanismen (wie etwa die Vorgabe zur Benennung eines Vertreters, wenn keine Niederlassung existiert) vorzusehen. Abs. 4 erstreckt den Anwendungsbereich des TTDSG auf Unternehmen in Drittstaaten außerhalb der EU, die in Deutschland Dienstleistungen erbringen. Bereits dieser weite Anwendungsbereich dürfte in der Praxis dazu führen, dass in Deutschland verfügbare Angebote von Drittstaatenunternehmen effektiv nicht wirksam kontrolliert und ggfs. sanktioniert werden können. Der Anwendungsbereich geht jedoch noch weiter und lässt bereits das „Mitwirken“ an Dienstleistungen ausreichen. Dies bedeutet, dass etwa der technische Dienstleister mit Sitz in Kanada eines Unternehmens aus den USA, welches Dienstleistungen in Deutschland erbringt, ebenfalls dem TTDSG unterliegt. Mit Blick auf die praktische Anwendung und Durchsetzung des Gesetzes ist fraglich, ob dies so gewollt ist.

Zudem lässt die Entwurfsbegründung offen, was mit den einzelnen Tatbestandsmerkmalen gemeint ist. Was bedeutet etwa das „Erbringen“ von Dienstleistungen? Ist hiermit mehr als ein reines „Anbieten“ gemeint? Zudem wird nicht beschrieben, welche Handlungen unter das „Mitwirken“ an Dienstleistungen fallen. Wir halten eine Klarstellung hierzu für erforderlich, um Rechtssicherheit und ein level-playing field zu ermöglichen.

Über die in § 1 genannten Abgrenzungen zum Anwendungsbereich ist generell im RegE festzustellen, dass sich einige Vorschriften explizit auf Anbieter öffentlicher Telekommunikationsdienste beziehen; andere Vorschriften knüpfen allgemein an die Anbieter von Telekommunikationsdienste an. Die nicht stringente Unterscheidung birgt die Gefahr, dass Vorgaben unbeabsichtigt auch auf unternehmensinterne Kommunikationslösung Anwendung finden. Insbesondere wenn innerhalb einer Unternehmensgruppe einem Unternehmen die gruppenweite Bereitstellung von internen Kommunikationstools übertragen wurde, besteht die Gefahr, dass dieser Anbieter von Telekommunikationsdiensten angesehen wird. Wir halten daher die Klarstellung für erforderlich, dass Unternehmen für interne Kommunikationsanwendungen nicht zum Telekommunikationsdienstleister werden.

b. § 2: Begriffsbestimmungen

Die enthaltenen Verweise, insbesondere auf die Definitionen der DS-GVO begrüßen wir. In § 2 Absatz 2 Nr. 4 ist für die Definition der „Nachricht“ noch die Beschränkung auf eine „endliche“ Zahl von Beteiligten enthalten. Diese Beschränkung wirft weiterhin Fragen auf, da die Gründe hierfür nicht unmittelbar ersichtlich sind. Eine Begründung hierzu hielten wir daher für hilfreich.

Die derzeitige Textfassung definiert die vom Gesetz erfassten Verkehrsdaten als solche, die "erforderlich" sind, abweichend von der früheren Definition in § 3 Nr. 30 TKG. Hier ist eine Klarstellung erforderlich, ob dies in Ansehung der nachfolgenden Regelungen tatsächlich so gemeint sein kann.
Bezüglich der Definition der Endeinrichtung stellt sich aus unserer Sicht die Frage, ob hiermit, insb. im Kontext des § 24 eigentlich eher “Endgeräte“ erfasst sein sollen. Dies wäre definitorisch dann klarzustellen.

Definitorisch ist aus unserer Sicht zudem eine Differenzierung zwischen Teilnehmern und Nutzern notwendig. Der Entwurf verwendet (überwiegend) den Begriff „Endnutzer“. Die fehlende Unterscheidbarkeit dürfte jedoch zu teils erheblichen Auswirkungen führen, etwa bei Erfüllung der Regelungen zur Einwilligung in die Verarbeitung von Verkehrsdaten

nach § 9 Abs. 2. Soweit demnach die Einwilligung des tatsächlichen Nutzers des Dienstes erforderlich ist, ist eine Einwilligung durch den Vertragspartner unter Umständen nicht mehr ausreichend und daher mit erheblichen Risiken verbunden. Das TTDSG sollte daher – wie das aktuelle TKG – generell eine Unterscheidung zwischen Teilnehmer und Nutzer vorsehen.

c. § 3: Vertraulichkeit der Kommunikation – Fernmeldegeheimnis

In § 3 halten wir einen Verweis auf § 164 TKModG und inhaltliche Kongruenz mit dem Sicherheitskatalog für erforderlich.

Darüber hinaus ist im Vergleich zum Referentenentwurf ist der vom Fernmeldegeheinmnis betroffenen Verpflichtetenkreis erheblich ausgeweitet worden. Beschränkte sich der Referentenentwurf noch auf Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze, sind vom Fernmeldegeheimnis nunmehr auch Anbieter nicht öffentlicher Dienste und Betreiber nicht öffentlicher Netze umfasst. Diese Ausweitung des Verpflichtetenkreises ist weder sachgerecht, noch steht sie in Übereinstimmung mit den europarechtlichen Vorgaben mit Art. 3 Abs. 1 und Art. 5 Abs. 1 ePrivacy Richtlinie iVm Art. 95 DSGVO.

Die ePrivacy Richtlinie stellt gemäß Art. 5 Abs. 1 die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Zudem gilt nach Art. 3 Abs. 1 die Richtlinie nur für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft. Eine Erstreckung des Fernmeldegeheimnisses auch auf nicht öffentliche, aber geschäftsmäßig erbrachte Telekommunikationsdienste und Netze stellt eine über-schießende Umsetzung der ePrivacy Richtlinie dar, die nach Art. 95 DSGVO aufgrund des Vorrangs der DSGVO unwirksam wäre.

Zudem ist die Einbeziehung von Anbietern von geschäftsmäßig angebotenen Telekommunikationsdiensten und von Betreibern von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden nicht angezeigt. Im TKG-E streicht der Gesetzgeber konsequent das Merkmal der „Geschäftsmäßigkeit“. Zudem wird auch die entsprechende Definition im TKG gestrichen. Eine Neuaufnahme im TTDSG ergibt insoweit keinen Sinn.

Gemäß § 3 Abs. 2 S. 1 TTDSG-E in der Fassung des Referentenentwurfs vom 12. Januar 2021 sollten nur Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze zur Wahrung des Fernmeldegeheimnisses verpflichtet sein.

Nach dem Regierungsentwurf vom 10. Februar 2021 sollen nun alle geschäftsmäßigen Anbieter von Telekommunikationsdiensten zur Wahrung des Fernmeldegeheimnisses verpflichtet sein, sodass die Regelung auch alle Arbeitgeber erfassen würde, die die Privatnutzung gestatten oder zumindest dulden.

Diese Erweiterung ist aus mehreren Gründen nicht angemessen, da die betroffenen Kommunikationsmittel im Verhältnis zwischen Arbeitgeber und Arbeitnehmer den Kommunikationszwecken des Arbeitgebers dienen und der Umstand, dass dieser ohne entsprechende Verpflichtung seinen Mitarbeitern die Privatnutzung der unternehmerischen Infrastruktur ermöglicht bzw. eine solche Nutzung zumindest duldet, sollte nicht dazu führen, dass dieser sich dem Risiko einer Strafbarkeit (§206 StGB) ausgesetzt sieht. Eine Einschränkung des Anwendungsbereichs des Fernmeldegeheimnisses ließe die betroffenen Arbeitnehmer dabei keineswegs schutzlos, da insbesondere die Vorschriften der DSGVO nach wie vor Anwendung fänden. Die Einschränkung erscheint auch vor dem Hintergrund angemessen, dass in Zeiten von Mobilfunk, Smartphones und mobilem Internet heutzutage kein Beschäftigter mehr auf die Nutzung betrieblicher Kommunikationsmittel für private Zwecke angewiesen ist.

d. Regelungen zum Digitalen Erbe in § 4 (Rechte des Erben des Endnutzers und anderer berechtigter Personen)

Angesichts der komplexen Fragen rund um das Thema „Digitales Erbe“ stellt sich hinsichtlich der bisherigen Regelung die Frage, welches Ziel hiermit genau erreicht werden soll und ob die in § 4 geregelte Klarstellung zur Verbesserung des derzeitigen Rechtsrahmens beiträgt und den Interessen der Kommunikationspartner des verstorbene ausreichend Rechnung trägt.

Wenn im Testament oder in einer Vollmacht nichts anderes geregelt ist, werden die Erben Eigentümer aller Gegenstände des Verstorbenen, also auch des Computers, Smartphones oder lokaler Speichermedien. Seit einem Urteil des Bundesgerichtshofs im Jahr 2018 beinhaltet dies auch den Zugang zu Accounts etwa in sozialen Medien. Damit dürfen die Erben die dort gespeicherten Daten uneingeschränkt lesen. Deshalb sollte man die Entscheidung, ob die Hinterbliebenen nach dem Tod Einblick in die digitale Privatsphäre haben, zu Lebzeiten treffen. Ein Notar oder Nachlassverwalter kann unter Umständen entsprechende Dateien oder ganze Datenträger vernichten bzw. konservieren lassen. Neben Hinweisen auf das Erbe können sich in persönlichen Dateien aber viele sensible private Informationen befinden.

Hinterbliebene erben nicht nur Sachwerte, sondern treten auch in die Verträge des Verstorbenen ein – auch, wenn es sich um kostenpflichtige Dienste handelt wie etwa ein Streaming-Abo. Gegenüber E-Mail- und Cloud-Anbietern haben Erben in der Regel Sonderkündigungsrechte. Bei der Online-Kommunikation gilt aber zugleich das Fernmeldegeheimnis, das auch die Rechte der Kommunikationspartner des Verstorbenen schützt. In der Praxis gelingt der Zugang zu den Nutzerkonten am besten, wenn der Verstorbene zu Lebzeiten geregelt hat, ob und in welchem Umfang die Erben im Todesfall Zugriff auf die Accounts erhalten. Außerdem können Nutzer die Zugangsdaten für solche Dienste beim Notar hinterlegen.

e. § 6: Regelung zur Nachrichtenübermittlung mit Zwischenspeicherung

Die neuen Regelungen aus dem EKEK und sowie die den EKEK umsetzenden Regelungen aus der TKG-Novelle erfassen nunmehr auch sogenannte OTT- Dienste. Die unterschiedlichen Funktionsweisen von „klassischen“ Telekommunikationsdiensten und OTT-Diensten werden mit der bisherigen Regelung aus unserer Sicht noch nicht ausreichend berücksichtigt. Der erfasste Anwendungsbereich ist zu unspezifisch und scheint sich ausschließlich an „klassischen“ TK-Diensten zu orientieren. OTT-Dienste sind häufig cloudbasierte Services, bei denen der Provider Kommunikationsinhalte für den Kunden verwaltet – zB im Fall von IMAP Postfächern beim E-Mail oder Messenger-Diensten. Es ist bei lebensnaher Auslegung hier grundsätzlich fraglich, ob es sich bei solchen service-immanenten Speichervorgängen tatsächlich um „Zwischenspeicherungen“ im Sinne des § 6 handeln soll, denn die Speicherung der Kommunikationsinhalte für den Nutzer hier ist in diesen Konstellationen geradezu eine Hauptleistung des beanspruchten Dienstes. Die Begründung geht hierauf bisher nicht ein, sodass wir eine Klarstellung für erforderlich halten, dass § 6 TTDSG entsprechenden servicetypischen Speichervorgängen bei interpersonellen Kommunikationsdiensten nicht entgegensteht.

§ 6 Absatz 2 sollte den Stand der Technik stärker einbeziehen und in klaren Zusammenhang mit dem Schutzzweck setzen. Wir schlagen daher vor, die letzten zwei Sätze zusammenzuführen und den Bezug zum Stand der Technik in direkten Kontext zu setzen: „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht und sie dem Stand der Technik entsprechen."

f. § 7: Verlangen eines amtlichen Ausweises

§ 7 bezieht sich inhaltlich auf die Identifikation des Endnutzers; dies sollte in der Überschrift entsprechend widergespiegelt werden. Wir schlagen daher vor, den § 7 mit „Identifizierung der Endnutzer" zu betiteln. Die Vorschrift des § 7 Absatz 2 ist darüber hinaus im Sinne eine kohärenten Regulierungsrahmens wie folgt anzupassen:

Statt "Der Endnutzer kann dazu den elektronischen Identitätsnachweis gemäß § 18 Personalausweisgesetz nutzen" sollte folgendes definiert werden:

"Der Endnutzer kann dazu einen elektronischen Identitätsnachweis mit dem Niveau "substanziell" oder "hoch" gemäß der Durchführungsverordnung (EU) 2015/1502 der EU Kommission nutzen".

Begründung: Damit eine möglichst große Gruppe von Endnutzern sich online ausweisen kann, muss die Gruppe der Online-Authentifizierungssysteme mindestens um die EU-Bürgerkarte gemäß eIDKG, die notifizierten Systeme auf dem Niveau "substanziell" oder "hoch" gemäß der Durchführungsverordnung (EU) 2015/1502 der EU Kommission und innovative Identifikationsmethoden gemäß § 11 VDG auf dem Niveau „substantiell" erweitert werden.

g. § 8 Missbrauch von Telekommunikationsanlagen

Zum bisherigen § 90 TKG gibt es in Europa keine vergleichbare Regelung. Dies führt gemeinsam mit den darin enthaltenen unbestimmten Rechtsbegriffen und dem Charakter als Strafvorschrift zu erheblichen Innovationshemmnissen und Wettbewerbsnachteilen für deutsche Unternehmen. Daher sollte die Überführung des § 90 TKG in den § 8 TTDSG zu einer Modernisierung und Anpassung der Vorschrift an die Chancen der Digitalisierung genutzt werden.

Mehr und mehr Arten von Geräten werden heute mit Kameras und Mikrofonen ausgestattet, um innovative Funktionen, wie z.B. Sprach- und Gestensteuerung, möglich zu machen. Dies entspricht Verbraucherwünschen und führt außerdem zu mehr Barrierefreiheit. In der vorgeschlagenen Form bringt § 8 jedoch erhebliche strafrechtliche Risiken für Anwender („besitzen“) und Anbieter solcher innovativer Technologien („auf dem Markt bereitstellen“, „einführen“). Unternehmen, die in Deutschland produzieren, sind darüber hinaus bei rein internationalem Vertrieb gegenüber ausländischen Wettbewerbern benachteiligt („herstellen“).

Kernproblem von § 8 stellt die große Unbestimmtheit der Begriffe verbunden mit einer Strafandrohung dar (Art. 80 GG). Das Schutzziel „Vertraulichkeit des Wortes“ wird im Übrigen bereits durch § 201 StGB umfassend geschützt. Etwaige Schutzlücken sollten im Strafgesetzbuch geschlossen und nicht unübersichtlich im Nebenstrafrecht geregelt werden.

Eine europäisch harmonisierte Regelung von Produkteigenschaften sollte der Vorzug gegeben werden. Diese wird in Kürze durch einen Delegated Act nach der Richtlinie 2014/53/EU Art. 3 (3) (e) erfolgen. Da diese Richtlinie zum neuen Konzept der Produktkonformität („New Legislative Framework“) gehört, kann dem technischen Fortschritt durch die Anpassung von Standards flexibel Rechnung getragen werden.

Falls dennoch an einer eigenständigen und europäisch nicht harmonisierten Beschränkung von Unternehmen in Deutschland festgehalten werden soll, so müsste § 8 zumindest so weit konkretisiert werden, dass keine erheblichen Risiken für Unternehmen in Deutschland drohen. Hierfür könnte man in Absatz 1 Satz 1 die Worte „geeignet und“ streichen. Außerdem sollte in Absatz 3 das Wort „nicht“ gestrichen und am Ende die Worte „oder dieser darauf hingewiesen wird.“

h. § 9 Verarbeitung von Verkehrsdaten

Die ePrivacy Richtlinie sieht in Art. 6 Abs. 1 vor, dass Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden. Die in der ePrivacy Richtlinie zusätzlich vorgesehene Anonymisierung statt Löschung fehlt in § 9 Absatz 1. Zur richtlinienkonformen Umsetzung ist daher in § 9 Absatz 1 der Satz „Im Übrigen sind

Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen“ um „oder zu anonymisieren“ zu ergänzen.

Dies ist auch im Einklang mit Art. 7 Abs. 2 des Entwurfs der ePrivacy Verordnung, der Betreiber eines elektronischen Kommunikationsdienstes verpflichtet, elektronische Kommunikationsmetadaten zu löschen oder zu anonymisieren, sobald sie für die Übermittlung einer Kommunikation nicht mehr benötigt werden.

Insgesamt zeigt die Umsetzung der Regelungen zur Verarbeitung von Verkehrsdaten im TTDSG, dass dringend eine Flexibilisierung der Verarbeitung von Kommunikationsmetadaten erforderlich ist. Der zuletzt von der portugiesischen Ratspräsidentschaft im Rahmen der ePrivacy Verordnung vorgeschlagene Möglichkeit zur Weiterverarbeitung von Kommunikationsmetadaten zu kompatiblen Zwecken ist ein Schritt in die richtige Richtung.

i. § 10 Entgeltermittlung und Entgeltabrechnung

In der derzeit vorgeschlagenen Form wird dies lediglich eine einfache Fortsetzung bestehender Gesetzgebung sein, die nicht ausreicht, um die Flexibilität zu ermöglichen, die notwendig ist, um eine verhältnismäßige und verantwortungsvolle Datennutzung durch Unternehmen zu ermöglichen. Demzufolge stellt sie eher ein Hindernis für datengesteuerte Innovationen dar, die für die Entwicklung der Digitalwirtschaft zwingend notwendig sind.

Es wird ein restriktiver Rahmen für die Verarbeitung von Kommunikations-Metadaten und Abrechnungsdaten aufrechterhalten, der nicht mit der DS-GVO übereinstimmt und nicht flexibel genug ist, um den Anforderungen zukünftiger Märkte gerecht zu werden. Um hier Abhilfe zu schaffen, schlagen wir vor, dass zumindest bei der Bereitstellung von Diensten für Unternehmenskunden der Grundsatz der kompatiblen Weiterverarbeitung im Einklang mit dem risikobasierten Ansatz der DS-GVO eingeführt wird.

j. 12 Störung von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

Der Novellierungsansatz, datenschutzrechtliche Anforderungen an die Erbringung elektronischer Kommunikationsdienste wie auch der Telemedien in einem Spezialgesetz zu konzentrieren, muss auf eine Kohärenz mit der DSGVO und dem EKEK sowie dem dazu

im Entwurf vorliegenden Telekommunikationsmodernisierungsgesetz achten. Dieses greift seinerseits nunmehr spezifische Anforderungen des IT SIG 2.0 auf und setzt diese insbesondere in § 164 um. Änderungen im Bereich der Telekommunikationsnovelle sind daher unbedingt auch im TTDSG-Entwurf zu berücksichtigen.

Im Ergebnis ist auch die Ergänzung in § 12 Abs. 4 abzulehnen, nach der die Verarbeitung von Verkehrsdaten zum Schutz der Endnutzer im Zusammenhang mit einer unzumutbaren Belästigung nach § 7 UWG ermöglicht wird. Es ist davon auszugehen, dass dies in eine Verpflichtung des Diensteanbieters zur Überprüfung der Inanspruchnahme der Telekommunikationsnetze- und Dienste auf Anforderung mündet oder sogar in einer Störer-Eigenschaft des Diensteanbieters, wenn diese unterbleibt. Diensteanbieter sähen sich einerseits den Aufforderungen der Betroffenen zur Unterbindung der angeblichen Belästigungen ausgesetzt und könnten diese andererseits schon aus Haftungsgründen nicht einfach unterbinden.

- Erlaubnis zur Datenverarbeitung für Systeme zur Angriffserkennung

§ 165 TKG-BT-E verpflichtet TK-Diensteanbieter Systeme zur Angriffserkennung zu betreiben, dies jedoch ohne eine Erlaubnis zur Datenverarbeitung vorzusehen. Eine solche Erlaubnis wäre nach der neu gewählten Systematik im TTDSG, insbesondere in § 12 TTDSG zu vermuten gewesen, fehlt aber auch hier. Um Systeme zur Angriffserkennung effektiv einsetzen zu können und auch sinnvolle Abwehr zu betreiben, ist es erforderlich, dass Verkehrs-, Steuer und Inhaltsdaten des Datenverkehrs nach Mustern und Indizien für Angriffe ausgewertet werden dürfen. Dies muss mittels sog. Intrusion Detection Systeme erfolgen.

Es ist daher entweder in § 12 TTDSG eine Erlaubnis zur entsprechenden Datenverarbeitung für die Zwecke des § 165 TKG-BT-E aufzunehmen oder klarzustellen, dass die entsprechende Verarbeitung nicht in Widerspruch zu § 4 und 10 TTDSG steht. Dies könnte geschehen, indem bei den vorgenannten Bestimmungen ein Zusatz beigefügt wird: „Unberührt bleibt die Nutzung von Verkehrs-, Steuer und Inhaltsdaten für Zwecke der Angriffserkennung und -abwehr."

k. Regelungen zu Teilnehmerverzeichnissen nach §17

Die Regelungen zu Teilnehmerverzeichnissen der § 45m und § 104 TKG wurden in § 17 TTDSG überführt und zusammengelegt. Hierdurch wird ohne erkennbaren Grund die

höchstrichterliche Rechtsprechung zur Differenzierung von Basisdaten und Zusatzdaten aufgehoben. Während die Eintragung von Basisdaten nach dem BVerwG für den Endnutzer unentgeltlich zu erfolgen hat, war die Eintragung von Zusatzdaten, die in der Regel der werblichen Darstellung des Endnutzers dienen, kostenpflichtig.

Hinsichtlich der Normadressaten muss § 17 TTDSG dringend präzisiert werden. Anspruchsgegner kann nur der Verzeichnisanbieter selbst sein und nicht der TK-Anbieter. Der TK-Anbieter kann nur den Wunsch des Endkunden, in ein Verzeichnis eingetragen zu werden, annehmen und diese Information Verzeichnisanbietern auf Nachfrage zur Verfügung stellen. Ebenso kann der TK-Anbieter den Wunsch des Kunden auf Löschung oder Korrektur an die Verzeichnisanbieter weiterleiten. Adressat für die Umsetzung der Eintragungs-, Korrektur- und Löschpflicht können nur die jeweiligen Verzeichnisanbieter sein, und nicht der jeweilige TK-Anbieter.

Über welches Medium ein Verzeichnis bereitgestellt wird, ist nicht relevant. Insofern kann der Normtext gekürzt werden und allgemein auf Verzeichnisse verwiesen werden. Die derzeitige Formulierung des § 17 Abs. 1 suggeriert, dass sowohl ein Anspruch des Endnutzers auf Eintragung in ein gedrucktes als auch ein elektronisches Verzeichnis bestehen könnte.

l. § 19 Technische und organisatorische Vorkehrung

Wir begrüßen, dass der Entwurf in § 19 Abs. 2 ausdrücklich auch weiterhin die anonyme und pseudonyme Nutzung von Daten ermöglicht (ausführlich dazu: Antworten zu Frage 4).

Aus unserer Sicht ist sprachlich eine Anpassung des § 19 notwendig, da er sich inhaltlich an den aus dem Datenschutzrecht bekannten technisch-organisatorischen Maßnahmen orientiert, hierzu aber von „technischen und organisatorischen Vorkehrungen“ spricht. Eine Einheitliche Bezeichnung würde aus unserer Sicht helfen, ein kohärentes Regelungssystem zu entwickeln.

m. § 20 Verarbeitung zum Zweck des Jugendschutzes

Die Regelung des § 20 lässt die Frage offen, ob von dem Verarbeitungsverbot auch solche Daten erfasst sein sollen, die durch Einwilligung erlangt wurden. Einer Doppelverwertung scheint uns in diesem Kontext nichts entgegenzustehen.

n. § 24: Regelung zur Einwilligung bei Endeinrichtungen

Die Regelung des § 24 wirft einige Fragen auf. So regelt der Entwurf beispielsweise nicht schlüssig das Verhältnis von § 24 TTDSG zur DSGVO, insb. Art. 6, 7 und 13. Sieht der Gesetzgeber in § 24 TTDSG eine Spezialregelung für den Vorgang des Zugriffs auf Informationen oder das Speichern von Informationen, unabhängig davon, ob es sich um personenbezogene Daten handelt? Wenn ja, würde die Zulässigkeit dieses Vorgang allein nach § 24 TTDSG und nicht nach Art. 6 Abs. 1 DSGVO beurteilt werden. Wenn die „Informationen" im Sinne des § 24 TTDSG auch personenbezogene Daten beinhalten, müsste dann daneben zusätzlich Art. 6 DSGVO beachtet werden?

Die Gesetzesbegründung zum § 24 TTDSG sollte aufgrund des weiten Anwendungsbereichs im Interesse aller vom Entwurf betroffener Anbieter wie folgt gefasst werden:

„Im Rahmen der vom Nutzer erwünschten Erbringung des Telemediendienstes ist auch das Speichern und Auslesen von Informationen auf Endeinrichtungen aus Sicherheitsgründen, einschließlich der Informationssicherheit und der Betrugsbekämpfung und aus sonstigen überwiegenden Interessen erforderlich und unterliegt nicht der Einwilligung durch den Endnutzer."

§ 24 greift weiterhin Regelungen auf, die zur Zeit auch im Rahmen der ePrivacy Verordnung vorgeschlagen und diskutiert werden. Wir sehen hier die Problematik, dass der Begriff der „Information" weder im EU-Recht noch im nationalen Recht legaldefiniert ist, weshalb z.B. nicht klar ist, ob etwa jegliche Softwareupdates künftig einer allgemeinen Einwilligungspflicht unterliegen, selbst wenn diese nichts an der Datenverarbeitung auf dem Endgerät ändern. Dies kommt in Betracht, weil für die Installation eines solchen Updates die Installationsdateien auf dem Endgerät des Nutzers gespeichert werden – würden diese Installationsdateien als „Informationen" im Sinne des § 24 TTDSG qualifizieren hätte die Norm eine allgemeine Einwilligungspflicht für Updates zur Folge.

Beispiel: Ein Automobilhersteller möchte ein Funktionsupdate des Park-Assistenten auf den Fahrzeugen eines bestimmten Typs over-the-air installieren, wobei das Update keinerlei Veränderung der Datenverarbeitung zur Folge hat.

Die Erfassung dieser Konstellationen durch § 24 TTDSG scheint nicht gewollt zu sein und wäre – u.a. mit Blick auf Sicherheitsupdates – auch eine hochproblematische Konsequenz der Norm. Wir halten daher eine Anpassung der Regelung für erforderlich.

Wir begrüßen jedoch, dass die aktuelle Fassung neben der Rechtsgrundlage der Einwilligung auch einwilligungslose Szenarien erfasst, in denen ein Zugriff auf das Endgerät "unbedingt erforderlich" für Erbringung des vom Nutzer gewünschten Dienstes ist. Diese Formulierung entspricht zum Einen den Vorgaben der Richtlinie, zum anderen lässt sie Spielraum für eine interessen- und nutzergerechte Interpretation. Auch eine vertragliche Grundlage, wie sie in der im Sommer 2020 bekannt gewordenen Fassung des TTDSG enthalten war, sollte aufgenommen werden.

Ausgehend von der Funktionsweise und Strukturen des Internets muss dies Maßnahmen einschließen können, die der Reichweitenmessung, Werbeblocker-Identifizierung, oder der Integritäts- und Sicherheitsüberprüfung zB auch durch Drittanbieter dienen. Die Erkennung der verwendeten Hardware und Software (insb. Browser) ist beispielsweise essentiell, da teilweise auf diese spezifischen Merkmale bei der Auslieferung von Webseiten eingegangen werden muss um eine fehlerfreie Darstellung gewährleisten zu können. In der Begründung sollte daneben auch die Klarstellung erfolgen, dass die Ausnahmen des § 24 auch Maßnahmen einschließen, die dem sog. Affiliate–Marketing dienen. Dieses Tracking mithilfe von Cookies ist die am meisten genutzte Methode, um einen User dem entsprechenden Affiliate zuordnen zu können, damit dieser so seine Vermittlung des Users vergütet bekommt. Wäre diese Nachverfolgung über Cookies nicht möglich, ginge der Affiliate leer aus.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.