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.

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).

bitkom

Einleitung

Am 12. Januar 2021 legte das Bundesministerium für Wirtschaft und Energie (BMWi) den Referentenentwurf für das Telekommunikations-Telemedien-Datenschutzgesetz (im Folgenden: TTDSG) vor. 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. Wir begrüßen zudem, dass die Entwicklung des TTDSG noch unter dem Vorbehalt der Änderung aufgrund parallel laufender Gesetzgebungsverfahren vorgenommen werden soll. 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.

Wir begrüßen daher auch, dass das BMWi neben der Verbändebeteiligung zum TTDSG einige angeschlossene Fragestellungen zur Diskussion stellt, auf die wir im Folgenden, ebenso wie zum Referentenentwurf des TTDSG, Stellung nehmen.

Detailkommentierung

1. **Frage 1: Im Zusammenhang mit der datenschutzrechtlichen Einwilligung und Verfahren zur praktikablen und nutzerfreundlichen Erteilung einer Einwilligung werden Regelungen zu Datenmanagementsystemen und „Personal Information Management-services— PIMS diskutiert. Der Gesetzentwurf enthält, insbesondere auch vor dem Hintergrund des Vorschlags der Europäischen Kommission zu sog. „data sharing services" im Rahmen des „Data Governance Act", eine solche Regelung nicht. Diesbezüglich werden die angeschriebenen Kreise um Rückmeldung gebeten, ob sie eine Regelung zu Datenmanagementsystemen/PIMs im TTDSG für erforderlich halten — und wenn ja, wie diese ausgestaltet sein soll.**

Der von der EU Kommission am 25. November vorgeschlagene Data Governance Act beinhaltet bereits Regelungen zu sogenannten Datenintermediären, den Datentreuhändern, die auch als Datenmanagementsysteme fungieren können. Zwar beinhaltet der Vorschlag bisher keine dezidierten Regelungen zu den Funktionsweisen und regelt daher bisher auch die möglichen Modelle von PIMS nicht unmittelbar. Wir halten es aber für das Gelingen der Datenökonomie und zur Stärkung des Vertrauens in Datenmittlersysteme für essentiell, dass auf harmonisierte, europäische Regelungen statt nationale Sonderregelungen gesetzt wird, um die Potenziale voll auszuschöpfen. Eine entsprechende Regelung ist unseres Erachtens daher derzeit weder erforderlich noch sinnvoll zu gestalten, da nicht absehbar ist wie der Data Governance Act final gestaltet sein wird. Im Ergebnis wird sich dieser datenschutzrechtlich jedoch an den Maßgaben der DS-GVO orientieren müssen, ebenso wie das TTDSG. Divergenzen zwischen den jeweiligen Rechtsnormen sind auch ohne einen Hinweis im TTDSG auf etwaige data sharing services nicht zu befürchten. Diese könnten sich jedoch ergeben, wenn ein Hinweis jetzt aufgenommen wird, der dem späteren Data Governance Act ggf. widerspräche.

Im derzeitigen Stadium sollte daher keine nationale Regelung im Kontext des TTDSG geschaffen werden. Stattdessen sollte sich das BMWi auf europäischer Ebene dafür einsetzen, dass für die PIMS ein EU-weiter Regelungsrahmen, zB mit dem Data Governance Act, geschaffen oder vorbereitet wird. Die hierfür im 2020 bekannt gewordenen Entwurf des TTDSG geregelten Vorschriften aus § 3 könnten hierfür als Vorbild für ein europäisches Rahmenwerk dienen.

2. **Frage 2: Das Bundesministerium für Wirtschaft und Energie spricht sich für die Einführung einer Regelung zu Browsereinstellungen im TTDSG aus, die verhindern soll, dass Browser herstellerseitig so eingestellt werden, dass der Zugriff auf die Informationen in Endeinrichtungen verhindert wird, auch wenn der Endnutzer eingewilligt hat. Im Hinblick auf eine solche Regelung werden die angeschriebenen Kreise ebenfalls explizit um Rückmeldung gebeten, ob Sie eine solche Regelung für sinnvoll erachten.**

Die Frage, ob und wie Browser Einwilligungen berücksichtigen können müssen, ist hoch relevant und aus technischer Sicht nicht trivial. Die hier aufgeworfene Frage betrifft daher auch verschiedene Dimensionen des Ökosystems der einwilligungsbasierten Datenverarbeitungen zwischen und über Webseiten und Browsern.

Der Referentenentwurf des TTDSG beinhaltet bislang keine Befolgungspflicht, durch die sichergestellt ist, dass erteilte Einwilligungen von Endnutzern gemäß § 22 effektive Wirkung entfalten. Die Einwilligung eines Nutzers oder auch Einstellungen des Nutzers über Personal Information Management Systemen sollten grundsätzlich Vorrang vor Softwareeinstellungen (beispielsweise von Browsern, Betriebssystemen oder anderen Voreinstellungen) haben.

Die aktuelle Entwicklungen des Marktes zeigt, dass Internetbrowser und andere Software zum Abrufen und Darstellen von Informationen aus dem Internet zunehmend den entsprechenden Datenzugang mitbeeinflussen: Durch Voreinstellungen der Software wird die Schnittstelle zwischen Endnutzern und Unternehmen, die Dienste anbieten, teilweise beschränkt – zB in Bezug auf die Möglichkeit der Platzierung sogenannter Third-Party-Cookies auf dem Endgerät des Nutzers. Diensteanbieter bzw. deren Partner werden dadurch in ihrer Interaktionsmöglichkeit mit dem Endgerät des Endnutzers beschränkt. Hierbei sind verschiedene Fallkonstellationen zu unterscheiden: Entsprechende Beschränkungen können bereits über die Voreinstellungen des Browsers hinterlegt sein oder aber erst durch den Nutzer aktiviert worden sein. Außerdem gibt es – von den Browserherstellern unabhängige – Anbieter entsprechender Plugins, die vom Nutzer aktiviert werden müssen.

Hierauf wird im Markt auf Publisher-Seite teile dergestalt reagiert, dass die Bereitstellung der jeweiligen Inhalte durch den jeweiligen Seitenbetreiber blockiert wird, soweit über den Browser oder Plugins entsprechende Beschränkungen ausgelöst werden.

Grundsätzlich ist der Fall vorstellbar, dass trotz einer beim Diensteanbieter vorliegenden individuellen Einwilligung nach § 22 iVm Art. 7 DS-GVO die Anbieter von Diensten (z.B.

einer Nachrichtenseite) nicht mehr zu den Endnutzern vordringen können und keinen vollständigen Zugriff auf gespeicherte Informationen zu erhalten bzw. die Möglichkeit solche Informationen zu hinterlegen (z.B. Cookies). Ebenfalls denkbar ist der Fall, dass Endnutzer bei der Nutzung eines Dienstes eine Einwilligung nach § 22 erteilen, diese jedoch keine Wirksamkeit entfalten kann, da die Softwareeinstellung diese bewusst erteilte Einwilligung unwirksam machen.

Wichtig ist, dass dieses Phänomen nicht alleine auf Internetbrowser beschränkt ist. Insbesondere in Hinblick auf mobile Endgeräte oder auch andere internetfähige Haushaltsgeräte (z.B. Fernsehgeräte) wird deutlich, dass die zum Abrufen und Darstellen von Informationen aus dem Internet eingesetzten Betriebssysteme und Softwareanwendungen den Datenaustausch beeinflussen können.

Es muss daher sichergestellt werden, dass unabhängig von den Einstellungen der Software die Anbieter der Dienste zu den Endnutzern vordringen können und erteilte Einwilligungen effektive Wirkung entfalten. Die Möglichkeit der Endnutzer zur Vornahme von Datenschutzeinstellungen an zentraler Stelle bleibt davon unberührt.

Eine Regelung in Form einer „Browserschranke“ wie sie für Art. 10 der vorgeschlagenen ePrivacy Verordnung diskutiert wurde ist vor diesem Hintergrund aber auch abzulehnen, da die damit verbundenen Rechts- und Sachfragen nicht geklärt sind. Auch im Kontext des Art. 10 wurde bereits angesprochen, dass die verpflichtende Positionierung von Browsern als "Kontrolleure" bereits starken technischen und rechtlichen Bedenken begegnet. Soweit Browser zentrale Steuerungsmöglichkeiten anbieten können sollen (oder nach den Vorschlägen der ePrivacy VO sogar verpflichtet werden sollen) ist technisch und rechtlich nicht geklärt, wie solche globalen Einstellungen durch individuelle Einstellungen (Einwilligung) auf Webseitenebene ergänzt werden können sollen.

Hierbei ist insbesondere die Problematik zu berücksichtigen, dass der Browserhersteller die Validität einer individuell zwischen Nutzer und Diensteanbieter bestehenden Einwilligung, deren inhaltliche Reichweite sowie das Nichtvorliegen eines Widerrufs nach DS-GVO schlicht nicht prüfen kann. Daher stellen sich im hier angedachten Modell insbesondere Fragen zu den etwaigen Anforderungen eines Einwilligungsnachweise zwischen Diensteanbieters und Browser, was auch Fragen der Identifizierung des jeweiligen Nutzers beinhalten würde, da die Einwilligung nur für den Nutzer wirken kann, der sie – gegenüber dem Diensteanbieter – erteilt hat.

Diese Fragen müssten vorab geklärt werden, vor allem, wie solch individuelle Einwilligungen validiert werden sollen. Dafür gibt es keine technischen Standards und

auch die Frage der (privacy/datenschutzrechtlichen) Verantwortlichkeiten ist nicht geklärt. Ein solcher Vorschlag bezieht sich daher auf ein Browser-Szenario welches a) noch in der politischen Diskussion ist um b) hieraus bereits vor Klärung von Sach- und Rechtsfragen weitere Verpflichtungen abzuleiten. Er ist aus unserer Sicht daher abzulehnen.

Zur weiteren Erörterung dieses wichtigen Themenkomplexes halten wir eine vertiefende Diskussion und Austausch für erforderlich. Bitkom steht hierfür jederzeit gern zur Verfügung.

3. **Frage 3: Das Bundesministerium des Innern spricht sich für die Aufnahme eine Regelung zum Ausschluss der Rufnummerunterdrückung für im Einzelfall festgelegte zentrale Rufnummern von Strafverfolgungsbehörden aus, um z. B. bei Anschlagsdrohungen oder erweiterter Suizidankündigung den Anschlussinhaber ermitteln zu können.**

Anbieter von Telekommunikationsdiensten müssen gem. § 66k (§ 119 TKG-neu KabE 2020) sicherstellen, dass beim Verbindungsaufbau als Rufnummer des Anrufers eine national signifikante Rufnummer übermittelt und als solche gekennzeichnet wird. Die Rufnummer muss dem jeweiligen Teilnehmer für diesen Dienst zugeteilt sein. Andere Anbieter, die an der Verbindung beteiligt sind, dürfen die übermittelte Rufnummer nicht verändern. Bei dieser Nummer handelt es sich um die sogenannte „network provided number“, über die der jeweilige Anrufer – etwa zu Abrechnungszwecken oder im Zusammenhang mit Belangen der öffentlichen Sicherheit (z. B. für den Notruf oder Überwachungsmaßnahmen) – identifizierbar sein soll. Zusätzlich wird die sog. „user provided number“ übermittelt, die von Nutzern entsprechend der gesetzlichen Vorgaben unterdrückt werden kann. Dies wirkt sich aber nicht auf die stets übertragende „network provided number“ aus.

Unseres Erachtens sollten daher die bestehenden Regelungen des bisherigen §108 Abs. 3 TKG (entspr. § 15 Abs. 1 Satz 4 TTDSG-Entwurf), die entsprechend und ergänzend auch für die Übermittlung von Standortdaten gilt (§ 13 Abs. 3 TTDSG-Entwurf) ausreichen, sodass wir eine zusätzliche Regelung für nicht notwendig erachten.

4. **Frage 4: Das Telemediengesetz (TMG) sieht in § 13 Abs. 6 derzeit vor, dass Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonymen zu ermöglichen haben, soweit dies technisch möglich und zumutbar ist. Eine Übernahme dieser Regelung ist in § 19 Abs. 2 TTDSG-Entwurf vorgesehen.**

   Das BMI und die Innenministerkonferenz des Bundes und der Länder (Beschluss-niederschrift der Frühjahrs-IMK Juni 2020 zu TOP 24) sprechen sich für gesetzliche Vorgaben zur Identifizierung zur Verifikation des Nutzers aus. Möglich wäre die Einführung einer entsprechenden Verpflichtung von Anbietern von Telemedien zur Erhebung und Verifizierung von Name, Adresse und Geburtsdatum nach dem Vorbild der bereits für Telekommunikationsdiensteanbieter geregelten entsprechenden Pflicht bei Prepaid-Mobilfunkdiensten § 111 Abs. 1 Satz 3 / § 171 Abs. 2 TKG-E. Dabei würde jeder Nutzer weiterhin selbst entscheiden können, ob er unter einem Pseudonym oder unter seinem Namen im Internet auftritt.

Die in Frage 4 in Bezug genommen Überlegungen der Innenministerkonferenz, einen faktischen Identifizierungszwang für sämtliche Telemedien (z.B. via Erhebungs- und Verifizierungspflicht für Mobilfunknummern) einzuführen lehnen wir strikt ab. Dies wäre ein grundlegender Paradigmenwechsel, der europaweit ohne Vorbild ist und auch europa und verfassungsrechtlich kaum durchsetzbar sein dürfte. Das Vertrauen in die Daten- und Digitalökonomie würde durch eine so weitreichende Pflicht eher gefährdet als gefördert. Ein entsprechender gesetzgeberischer Vorstoß ließe sich aus unserer Sicht nur dann diskutieren, wenn die betroffenen und perspektivisch eingeschränkten Grundrechte transparent genannt, die Ziele klar kommuniziert und die Verbesserung für den Bereich der Strafverfolgung spezifiziert würden. Die Zielerreichung des Vorschlags steht ansonsten grundsätzlich in Frage. Auch aus Gründen des Wettbewerbs sprechen wir uns gegen den Vorschlag aus, da eine solche Regelung zu gravierenden Wettbewerbsnachteilen für deutsche Unternehmen im Vergleich zu anderen EU-Staaten führen dürfte, in denen keine Verifikation erforderlich/durchsetzbar ist. Eine Verpflichtung zur Verifikation hätte zudem weitere datenschutzrechtliche Pflichten zur Folge, deren Einhaltung zu einem immensen Folgeaufwand führen würde, da die Nutzer durch die Verifikation identifizierbar sind (z.B. Gewährleistung des Rechts auf Auskunft und Datenlöschung). Teils dürfte eine Verifizierung von Nutzern aber auch schlicht unmöglich sein, etwa wenn sich ein Nutzer im Ausland befindet.

Die Umsetzung dieses Vorschlags hätte zudem zur Folge, dass beispielsweise sämtliche deutsche Nutzer von E-Mail-Konten diese künftig nur noch nutzen könnten, wenn sie sich gegenüber ihrem Provider identifizieren und ihre Identität verifizieren. Gleiches gilt für sämtliche anderen Online-Dienste.

In der Folge stünde zu erwarten, dass sich die heute schon im Millionenbereich bewegenden Abfragen über die automatisierte Bestandsdatenabfrage für Mobilfunknummern nach § 112 TKG stark erhöhen würde.

Eine solche Regelung zur Identifizierung sämtlicher Nutzer die Betreiber von entsprechenden Diensten vor erhebliche zusätzliche administrativen Aufwand stellen, da entsprechende Systeme zur Verifizierung und Speicherung der Identität eingeführt werden müssten.

Effektive Strafverfolgung ist auch im digitalen Kontext ein wichtiges Thema. Der Bitkom hält aufgrund der Komplexität und Vielschichtigkeit des Themas jedoch einen vertieften, Ressort- und stakeholderübergreifenden Dialog für dringend erforderlich. Für einen solchen Austausch steht der Bitkom jederzeit zur Verfügung.

5. Detailkommentierung zum Referentenentwurf 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. 4 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 RefE 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 gegenüber dem im Sommer 2020 bekannt gewordene Entwurf des TTDSG nun enthaltenen Verweise, insbesondere auf die Definitionen der DS-GVO begrüßen wir (jedoch kann aufgrund des nun eingefügten Verweises die zusätzliche Verweisung in § 22 Abs. 1 Satz 2 entfernt werden). In § 2 Absatz 2 Nr. 3 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 § 22 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.

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.

§ 12 lässt eine solche harmonisierte Umsetzung jedoch – in mindestens zwei zentralen Punkten – vermissen:

- Steuerdaten

Im Zusammenhang mit Störungen ermöglich § 12 Abs. 1 nur noch die Verarbeitung von Verkehrsdaten. Die in § 100 Abs. 1 TKG genannten Steuerdaten wurden nicht in den Entwurf übernommen. Damit führt § 12 Abs. 1 zu einer nicht erforderlichen Einschränkung des Rechts des Anbieters bzw. Betreibers auf Störungsbekämpfung.

Die in § 12 Abs. 2 aufgenommene Berichtspflicht gegenüber dem BfDI ist nunmehr nicht auf automatisiert erhobene Daten (vgl. § 100 Abs. 1 S. 5 und 6 TKG) beschränkt, sondern betrifft sämtliche Entstörungsmaßnahmen. Die Verpflichtung würde zu einem deutlich höheren, unverhältnismäßigen Dokumentationsaufwand führen.

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 aufs Haftungsgründen nicht einfach unterbinden.

- Erlaubnis zur Datenverarbeitung für Systeme zur Angriffserkennung

§ 164 TKG-RefE 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 § 162 TKG-RefE 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. § 13 Standortdaten

In § 13 Abs.3 halten wir eine Klarstellung hinsichtlich der Notrufverpflichtungen auf dem TKG für erforderlich.

l. Regelungen zu Teilnehmerverzeichnissen nach §§17,18

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.

Darüber hinaus dient § 18 TTDSG der Umsetzung von Artikel 112 EU-Richtlinie 2018/1972. Diese sieht vor, dass die Bereitstellung der Daten nicht kostenlos, sondern kostenorientiert zu erfolgen hat. Die Aufbereitung der Daten ist mit Aufwänden verbunden, weshalb für die Überlassung der Endnutzerdaten an die Herausgeber von Auskunfts- und Verzeichnismedien Anbieter von Kommunikationsdiensten berechtigt sein sollten, ein kostenorientiertes Entgelt zu erheben.

Konkret sollten die Regelungen wie folgt angepasst werden:

Endnutzerverzeichnisse, Bereitstellen von Endnutzerdaten
§ 17 Endnutzerverzeichnisse
(1) Inhaber von Teilnehmeranschlüssen können mit ihrer **Rufnummer** ~~**Anschlusskennung**~~, ihrem Namen, ihrer Anschrift ~~**und zusätzlichen Angaben wie Beruf, Branche und Art des Anschlusses**~~ in ~~**gedruckte oder elektronische**~~ **Endnutzerv**~~**V**~~erzeichnisse, die der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglich sind, eingetragen werden, soweit sie dies beantragen. Dabei können die Antragsteller bestimmen, welche Angaben in den Verzeichnissen veröffentlicht werden sollen. Auf Verlangen des Antragstellers dürfen weitere Nutzer des Teilnehmeranschlusses mit Namen und Vornamen eingetragen werden, soweit diese damit einverstanden sind. Für die Einträge nach Satz 1 darf ein Entgelt nicht erhoben werden.

(2) Der Anbieter eines nummerngebundenen interpersonellen Telekommunikationsdienstes hat den Endnutzer bei der Begründung des Vertragsverhältnisses über die Möglichkeit zu informieren, seine Rufnummer, seinen Namen, seinen Vornamen und seine Anschrift in ~~**gedruckten oder elektronischen**~~ Verzeichnissen, die der Öffentlichkeit unmittelbar oder über Auskunftsdienste zugänglich sind, aufzunehmen.

(3) Der Endnutzer eines nummerngebundenen interpersonellen Telekommunikationsdienstes kann von seinem Anbieter jederzeit verlangen, **dass** ~~**mit**~~ seine~~**r**~~ Rufnummer, sein~~**em**~~ Name~~**n**~~, sein~~**em**~~ Vorname~~**n**~~ und seine~~**r**~~ Anschrift **zum Zwecke der Veröffentlichung in Auskunfts- und Verzeichnismedien gespeichert und gemäß § 18 TT-DSG zur Verfügung gestellt werden. Der Endnutzer kann bei seinem Anbieter einen Antrag auf Berichtigungen oder Löschungen der gespeicherten Daten stellen.** ~~**in ein allgemein zugängliches, nicht notwendig anbietereigenes Endnutzerverzeichnis unentgeltlich eingetragen zu werden oder seinen Eintrag wieder löschen zu lassen.**~~ **Anbieter von Auskunfts- und Verzeichnisdiensten sind verpflichtet, die gemäß § 18 TTDSG übermittelten Daten zu veröffentlichen sowie unrichtige oder gelöschte Daten aus den Verzeichnissen zu entfernen und Berichtigungen vorzunehmen.** ~~**Einen unrichtigen Eintrag hat der Anbieter zu berichtigen.**~~

§ 18 Bereitstellen von Endnutzerdaten

(1) Jeder Anbieter eines nummerngebundenen interpersonellen Telekommunikationsdienstes hat unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen jedem Unternehmen auf Antrag Endnutzerdaten nach § ~~**14**~~ **17** Absatz ~~**1**~~ **3** zum Zwecke der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten, Diensten zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers und von Endnutzerverzeichnissen bereit zu stellen.

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

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

(4) Die nach Absatz 2 bereit gestellten Daten müssen vollständig sein und inhaltlich sowie technisch so aufbereitet sein, dass sie nach dem jeweiligen Stand der Technik ohne Schwierigkeiten in ein kundenfreundlich gestaltetes Endnutzerverzeichnis oder eine entsprechende Auskunftsdienste-Datenbank aufgenommen werden können.

Begründung der Ergänzung in Absatz 3: Die Vorschrift dient der Umsetzung von Art. 112 EU-Richtlinie 2018/1972. Diese sieht vor, dass die Bereitstellung der Daten nicht kostenlos, sondern kostenorientiert zu erfolgen hat. Insofern dient der Änderungsvorschlag der Umsetzung der Richtlinie. Die Aufbereitung der Daten ist mit Aufwänden verbunden, weshalb für die Überlassung der Endnutzerdaten an die Herausgeber von Auskunfts- und Verzeichnismedien Anbieter von Kommunikationsdiensten berechtigt sein sollten, ein kostenorientiertes Entgelt zu erheben.

m. § 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.

n. § 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. Eine Doppelverwertung scheint uns in diesem Kontext nichts entgegenzustehen.

o. § 22: Regelung zur Einwilligung bei Endeinrichtungen

Die Regelung des § 22 wirft einige Fragen auf. So regelt der Entwurf beispielsweise nicht schlüssig das Verhältnis von § 22 TTDSG zur DSGVO, insb. Art. 6, 7 und 13. Sieht der Gesetzgeber in § 22 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 § 22 TTDSG und nicht nach Art. 6 Abs. 1 DSGVO beurteilt werden. Wenn die „Informationen“ im Sinne des § 22 TTDSG auch personenbezogene Daten beinhalten, müsste dann daneben zusätzlich Art. 6 DSGVO beachtet werden? Aus unserer Sicht spricht das Urteil des EuGH in der Sache Planet49 eher für eine Spezialregelung, da der EuGH die Anforderungen des Art. 5 Abs. 3 RL 2002/58/EG unabhängig davon prüft, ob

personenbezogene Daten betroffen sind oder nicht. Zumindest in der Begründung zu § 22 TTDSG sollte es hierzu eine Klarstellung geben.

In der Begründung des Entwurfs sind bisher dezidierte Erläuterungen zum Bereich des automatisierten und vernetzten Fahrens enthalten. So soll der Endnutzer, also der Fahrer oder Fahrzeugeigentümer, das Speichern oder Auslesen von Informationen auf Endeinrichtungen im Fahrzeug zu dulden haben, da dies aus Sicherheitsgründen erforderlich ist (Gesetzesbegründung zu § 22 TTDSG, Seite 33 Mitte). Die hier richtigerweise getätigte Abwägung und Berücksichtigung von Sicherheitsinteressen darf nicht nur auf den in der Begründung erwähnten Sachverhalt Anwendung finden, sondern ist vielmehr zu verallgemeinern. Die Gesetzesbegründung ist daher im Interesse aller vom Entwurf betroffener Anbieter wie folgt zu fassen:

„Ist das Speichern und Auslesen von Informationen auf Endeinrichtungen aus Sicherheitsgründen, einschließlich der Informationssicherheit und der Betrugsbekämpfung und aus sonstigen überwiegenden Interessen erforderlich, unterliegt es nicht der Bestimmung durch den Endnutzer."

§ 22 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 § 22 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 § 22 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 § 22 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.

p. § 25: Zuständigkeit, Aufgaben und Befugnisse des BfDI

Während wir eine stärkere Harmonisierung der Datenschutzaufsicht für notwendig erachten,[1] sehen wir bei der derzeitigen Zuständigkeitszuweisung die Gefahr der Dopplung von Zuständigkeiten, insbesondere im Verhältnis zur BNetzA und den nach der DS-GVO zuständigen federführenden Datenschutzaufsichtsbehörden in anderen EU-Mitgliedstaaten.

Die mit § 25 Abs. 2 vorgenommene neue Zuständigkeitszuweisung der Einhaltung des § 22 für TK-Unternehmen an den BfDI ist aus zweierlei Gesichtspunkten abzulehnen. Zum einen erfolgt bisher eine Auftrennung der Zuständigkeiten zwischen BfDI und LfDI branchenbezogen. Die Zuständigkeit des BfDI besteht für Post und Telekommunikation und für Bundesbehörden. Nunmehr soll hierzu auch noch eine inhaltliche Komponente der Einhaltung der Vorgaben des § 22 kommen. Dies passt systematisch nicht in die Zuständigkeitsaufteilung. Zudem wird eine derartige Zuständigkeitszuweisung zu ganz erheblichen Abgrenzungsproblemen mit der Zuständigkeit der LfDI führen. Hier müsste eine genaue Abgrenzung vorgenommen werden, wann ein Speichern von Informationen in den Einrichtungen der Endnutzer technisch beginnt und damit auch die Zuständigkeit des BfDI und wann eine Datenverarbeitung von Kundedaten und Daten von

[1] Ausführlich dazu hier: https://www.bitkom.org/Bitkom/Publikationen/Struktur-der-Datenschutzaufsichtsbehoerden-in-Deutschland

Websitenutzern erfolgt, die nicht unter § 22 fällt, für die dann wiederum der LfDI zuständig wäre. Die Regelung in § 25 Abs. 2 wird das Zuständigkeitsdickicht eher vergrößern, als denn verringern.

Es ist zugleich in jedem Fall klarzustellen, dass der BfDI die Aufsicht nur im Hinblick auf seinen Zuständigkeitsbereich (insbes. Bundesbehörden, TK-Unternehmen) durchführt. Andernfalls wären Unternehmen gezwungen sich für einen kleinen Teilbereich des Datenschutzrechts (zusätzlich) an eine andere Behörde (den BfDI) zu wenden. Es würde dabei ein einheitlicher Lebenssachverhalt auf mehrere Behörden aufgeteilt werden: Z.B. wäre bei Cookies für das Setzen oder Auslesen der BfDI zuständig. Dagegen wären die Einwilligung, die Datenschutzerklärung etc. mit der jeweiligen Landesbehörde abzustimmen. Eine solche Zuständigkeitszersplitterung führt also nicht nur zu Mehraufwand bei den Unternehmen, sondern auch zu Rechtsunsicherheit. Dies kann nicht im Interesse des Gesetzgebers sein, der einen wirksamen Datenschutz anstrebt.

Im Übrigen muss es hinsichtlich der datenschutzbezogenen Regelungen bei der Zuständigkeit der Landesbehörden bleiben.