Deutscher Bundestag
19. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 19(9)1043
20. April 2021

TH Köln · Gustav-Heinemann-Ufer 54 · 50968 Köln

Deutscher Bundestag
Ausschuss für Wirtschaft und Energie
Platz der Republik 1
11011 Berlin

Kölner Forschungsstelle
für Medienrecht

Technology
Arts Sciences
TH Köln

Stellungnahme

von

Professor Dr. Rolf Schwartmann

im Rahmen der öffentlichen Anhörung
des Ausschusses für Wirtschaft und Energie
des Deutschen Bundestages

zum

Entwurf eines Gesetzes
zur Regelung des Datenschutzes und
des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)
(BT-Drucksache 19/27441)

Berlin, 21. April 2021

Prof. Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht
+49 221-8275-3446
medienrecht@th-koeln.de
www.medienrecht.th-koeln.de
Claudiusstraße 1
50678 Köln

Technische Hochschule Köln

Postanschrift:
Gustav-Heinemann-Ufer 54
50968 Köln

Sitz des Präsidiums:
Claudiusstraße 1
50678 Köln

www.th-koeln.de

Kölner Forschungsstelle
für Medienrecht

Leitung:
Prof. Dr. Rolf Schwartmann

Inhaltsverzeichnis

Teil 1: Zusammenfassung 3

Teil 2: Stellungnahme zum Gesetzesentwurf im Einzelnen..... 4

1. Cookies und Nutzererkennung..... 4

a) Konkretisierende Regelbeispiele zur „unbedingten Erforderlichkeit“ 5

b) Verhältnis von § 24 TTDSG-E zur DS-GVO 5

2. Dienste zur Einwilligungsverwaltung 6

a) Dringender Anlass einer nationalen Regelung..... 6

b) Regelungsziel..... 7

c) Funktionsweise von Diensten zur Einwilligungsverwaltung..... 7

d) Anforderungen an Dienste zur Einwilligungsverwaltung 9

3. Geltung des Fernmeldegeheimnisses für die Privatnutzung gestattende Arbeitgeber (§ 3 TTDSG-E)..... 10

4. Gebot der anonymen und pseudonymen Nutzbarkeit von Telemedien (§ 19 Abs. 2 TTDSG-E)..... 11

Teil 1: Zusammenfassung

1. Das Tatbestandsmerkmal der **unbedingten Erforderlichkeit** bei fehlendem Einwilligungserfordernis (§ 24 Abs. 1 Nr. 2 TTDSG-RegE) bei **Cookies und Nutzererkennung** ist durch Regelbeispiele zu konkretisieren. Nur so kann das gesetzgeberische Ziel zur Schaffung von Rechtssicherheit erreicht werden. Dies betrifft insbesondere die Reichweitenmessung.

2. Die Einführung eines geeigneten Rechtsrahmens für **Dienste zur Einwilligungsverwaltung (PIMS)** und dessen adäquate Ausgestaltung sind zur effektiven und verbindlichen Durchsetzung des Verbraucherwillens essentiell.

3. Die Geltung des **Fernmeldegeheimnisses** europarechtskonform auf Anbieter für die Öffentlichkeit zu beschränken (§ 3 TTDSG-E). Arbeitgeber die Beschäftigten Privatnutzung von dienstlichen Kommunikationsmitteln gestatten, gehören nicht dazu.

4. Das Gebot der anonymen und **pseudonymen Nutzbarkeit** von Telemedien (§ 19 Abs. 2 TTDSG-E) ist auf die pseudonyme Nutzbarkeit zu beschränken. Anonyme Nutzung ist faktisch ausgeschlossen.

Teil 2: Stellungnahme zum Gesetzesentwurf im Einzelnen

Der Bundestag hat mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) die Chance, wichtige Weichen für den Datenschutz in der elektronischen Kommunikation zu stellen. Die Konsolidierung und Zusammenführung der Datenschutzvorgaben für Telemedien- und Telekommunikationsdienste sowie deren Angleichung an das geltende europäische Recht sind Kernanliegen des TTDSG.[1] Dies ist wichtig, weil das Nebeneinander von DS-GVO, TMG und TKG bei Anbietern wie Verbraucher/innen zu Rechtsunsicherheiten führt. Angesichts der Differenzen zwischen Rat und Europäischem Parlament sollte auch der Abschluss des Verfahrens zum Erlass einer ePrivacy-Verordnung nicht länger abgewartet werden. Sein Ziel erreicht der aktuelle Gesetzentwurf bislang allerdings nur teilweise. Um seine Regelungswirkung zu entfalten und Rechtssicherheit für Nutzer/innen und Onlinewirtschaft gleichermaßen zu erzeugen, sind Anpassungen erforderlich.

Zwei Punkte sind **essentiell**:

1. Die Konkretisierung des Tatbestandsmerkmals der **unbedingten Erforderlichkeit** bei fehlendem Einwilligungserfordernis (§ 24 Abs. 1 Nr. 2 TTDSG-RegE) bei **Cookies und Nutzererkennung**.

2. Die Einführung eines geeigneten Rechtsrahmens für **Dienste zur Einwilligungsverwaltung (PIMS)** und dessen adäquate Ausgestaltung.

Zwei weitere Punkte sind wichtig:

3. Geltung des **Fernmeldegeheimnisses** für die Privatnutzung gestattende Arbeitgeber (§ 3 TTDSG-E)

4. Gebot der anonymen und **pseudonymen Nutzbarkeit** von Telemedien (§ 19 Abs. 2 TTDSG-E)

Im Einzelnen:

1. Cookies und Nutzererkennung

Wichtige Praxisfragen im Zusammenhang mit Cookies und vergleichbaren Verfahren bleiben nach der geplanten Regelung, die sich unmittelbar am Wortlaut der ePrivacy-Richtlinie orientiert, ungelöst.[2] Dies gilt etwa im Hinblick auf Cookies, die zur Websiteoptimierung (auch „Reichweitenmessung“ oder „Analytics“) zum Einsatz kommen. Die Abhängigkeit von einer

[1] Dazu *Schwartmann/Benedikt/Reif*, Entwurf zum TTDSG: Für einen zeitgemäßen Datenschutz MMR 2021, 99 ff.; *dies*. Datenschutz bei Websites – aktuelle Rechtslage und Ausblick auf das TTDSG, RDV 2020, 231 ff.

[2] Zur Problematik und Komplexität der unbefriedigenden der Rechtslage im Spannungsfeld zwischen EPrivacy-Richtlinie, TMG und DS-GVO in der Rechtsprechung von EuGH und BGH unter Berücksichtigung der Auslegungspraxis der DSK vgl. *Schwartmann/Klein* in *Schwartmann/Jaspers/Thüsing/Kugelmann*, DS-GVO/BDSG (2. A. 2020), Art. 6 Rn. 172 ff.

Nutzereinwilligung ist problematisch, weil eine effektive Websiteoptimierung eine möglichst breite Datenbasis, eine wirksam erteilte Einwilligung aber deren Freiwilligkeit bedingt.

First-Party-Analyse-Cookies stellen zudem **kein** nennenswertes **Datenschutzrisiko** dar, wenn sie nur für aggregierte Statistiken des Erstanbieters genutzt und nach transparent von Websites verwendet werden.[3] § 24 Abs. 2 Nr. 2 TTDSG-RegE stellt als Ausnahme vom Einwilligungserfordernis darauf ab, ob die Speicherung der Information im Endgerät oder ein Zugriff darauf „unbedingt erforderlich" zur Diensterbringung ist. Ob etwa **Cookies zur Websiteoptimierung** darunter fallen, ist nicht eindeutig.[4]

Da die Zulässigkeit des Einsatzes von Cookies und vergleichbaren Technologien einer der Dreh- und Angelpunkte des TTDSG und zugleich von immenser Relevanz für Nutzer/innen und Wirtschaft ist, sollte dieser Punkt dringend konkretisiert werden. Nur so kann das Ziel des Gesetzentwurfs, bestehende Rechtsunsicherheiten zu beseitigen, erreicht werden.

a) Konkretisierende Regelbeispiele zur „unbedingten Erforderlichkeit"

Zielführend ist es, **Regelbeispiele** in den Gesetzestext aufzunehmen, bei deren Vorliegen davon ausgegangen werden kann, dass die unbedingte Erforderlichkeit zu bejahen ist. Konkret zu nennen, sind etwa die Bereiche:

- Warenkorb- und Session-Cookies
- Vorhalten von Nutzerpräferenzen (wie z.B. Sprach- und Bildschirmeinstellungen)
- Verfahren zur Reichweitenmessung
- Gewährleistung zur technischen Sicherheit und Integrität der Website
- Websiteoptimierung.[5]

Nur so kann die Norm den Anforderungen der rechtsstaatlich erforderlichen **Bestimmtheit und Normenklarheit** gerecht werden. Ohne die Konkretisierung des unbestimmten und konturenlosen, aber für Verbraucher/innen und Wirtschaft zentralen Rechtsbegriffs, ist dessen Auslegung insbesondere auch Aufsichtsbehörden und Gerichte nicht sicher möglich. Es bedarf also dringend eines tauglichen gesetzlichen Rahmens.

Notfalls müsste alternativ der Weg über eine Verordnungsermächtigung zur Durchführung der Konkretisierung, jedenfalls aber auch die Gesetzesbegründung erfolgen.

b) Verhältnis von § 24 TTDSG-RegE zur DS-GVO

Entsprechend den Vorgaben der ePrivacy-Richtlinie soll § 24 TTDSG-E unabhängig davon gelten, ob bei dem Zugriff auf die Endeinrichtung personenbezogene Daten anfallen. Unklar ist, ob § 24 TTDSG-E dennoch in dem Fall, dass mit dem Zugriff auf die Endeinrichtung

---

[3] *Art. 29-Datenschutzgruppe*, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, Stand: 7.6.2012, S. 11 f.

[4] Zur Rechtsunsicherheit bei der Einordnung „technisch notwendiger Cookies" bereits *Schwartmann/Benedikt/Reif*, RDV 2020, 231 ff., *Schwartmann/Klein* in *Schwartmann/Jaspers/Thüsing/Kugelmann*, DS-GVO/BDSG (2. A. 2020), Art. 6 Rn. 172 ff.

[5] Zu Letzterem vgl. *CNIL*, Délibération no 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs).

personenbezogene Datenverarbeitungen einhergehen, auch Rechtsgrundlage für diese personenbezogene Datenverarbeitung sein soll. Hierzu wäre eine Klarstellung in der Gesetzesbegründung wünschenswert.

2. Dienste zur Einwilligungsverwaltung

a) Dringender Anlass einer nationalen Regelung

Der Gesetzentwurf sollte daher wieder um eine Regelung zu **Personal Information Management Services (PIMS)** ergänzt werden. Neben einem erstrebenswerten hohen Datenschutzstandard sorgt ein fehlender Rechtsrahmen für PIMS derzeit für große Rechtsunsicherheit in Unternehmen, die Datenschutzmanagementsysteme entwickeln oder einsetzen möchten, wie es der Bundesrat in seiner Stellungnahme zum TTDSG bereits ausgeführt hat.[6]

Die Empfehlung zur Einführung dieser PIMS hat die **Datenethikkommission** (DEK) ausgesprochen, die Datenmanagement- und Datentreuhandsystemen ein großes Potenzial attestiert.[7] Die Idee ist, dass Nutzer auf Dashboards Datenschutzeinstellungen vornehmen, die von den Diensteanbietern übernommen werden müssen. So soll zudem insbesondere eine **„Click Fatigue“**, die aus dem ständigen Wegklickenmüssen von Cookie Bannern resultiert, verhindert werden. Ohne eine entsprechende Regelung der PIMS hätte das TTDSG den unbeabsichtigten Nebeneffekt, dass durch massenhaft abgefragte Einwilligungen die gesellschaftliche Akzeptanz für den Datenschutz insgesamt schwindet.[8]

Datentreuhänder können hier eine **wichtige Funktion** einnehmen, indem sie Datenschutzeinstellungen speichern und für angeschlossene Telemediendienste eine Schnittstelle zum Abruf dieser Einstellungen bieten. Eine gesonderte Einwilligung des Nutzers für den jeweiligen Telemediendienst kann hierdurch entfallen. Auf diese Weise könnten wir zeitnah, effizient und mit wenig Aufwand eine Lösung finden. Damit würde eine plattformneutrale Lösung geschaffen und so Wettbewerb ohne Cookies für alle Marktteilnehmer ermöglicht.

Das ursprüngliche Vorhaben mit Blick auf den auf europäischer Ebene geplanten **Data Governance Act (DGA**) zurückzustellen, überzeugt nicht. Der DGA hat eine ganz andere Zielrichtung als das TTDSG durch die Schaffung eines echten europäischen Marktes für Daten mittels entsprechender Datenräume.[9] Die Regelung zu Datenintermediären in Art. 9 Abs. 1 lit. b des Kommissionsentwurfs erfasst zwar nominal auch Dienste zur Einwilligungsverwaltung, hat aber den Fokus auf Betroffenen, die ihre Daten einem Datennutzer aktiv zur Verfügung stellen.

---

[6] Vgl. BR-Drucks. 163/21 (Beschluss) vom 26.03.2021, S. 12.
[7] Gutachten der *Datenethikkommission (2019)*, Empfehlung 21.
[8] *Schwartmann/Hanloser/Weiß*, Kurzgutachten zu PIMS im TTDSG - Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, März 2021, S. 2.
[9] Vgl. ErwG 2 DGA.

Das **Stocken des ePrivacy-Prozesses** zeigt, wie wichtig **Impulse aus den Mitgliedstaaten** für die europäische Regulierung sind. Hier sollte Deutschland seine Rolle als Impulsgeber wahrnehmen. Allerdings macht am Ende nur eine einheitliche europäische PIMS-Regelung Sinn. Deshalb sollte der deutsche Gesetzgeber sich im TTDSG am Entwurf des Art. 11 Data Governance Act v. 25.11.2020 orientieren und keine geringeren Anforderungen an PIMS formulieren.

b) Regelungsziel

Die **Deutungshoheit und Kontrolle** über die Verwendung von Daten muss und kann im TTDSG gerechter verteilt werden. **Belästigende, sich wiederholende Cookie-Banner** sind im Interesse von Nutzer/innen mithilfe **datenschutzfreundlicher Technologien** weitgehend zu reduzieren. Das gesetzliche Mittel hierzu ist die Verankerung eines sogenannten Einwilligungsmanagementsystems (Personal Information Management Systems, PIMS) im TTDSG. Staatlich anerkannte Dienste könnten als unabhängige Treuhänder zwischen Nutzer/innen und digitalen Diensten stehen. Deren Aufgabe wäre es, nach offenen Standards Einwilligungen zu verwalten. Ergänzende Dienste wie die Verwaltung eines Zugangs (Log In) zu Online-Diensten sind denkbar.

c) Funktionsweise von Diensten zur Einwilligungsverwaltung

Die **Dienste zur Einwilligungsverwaltung** würden als eine **Spielart des Datentreuhänders**[10] Kunden mit Unternehmen verbinden, indem nur die Weiterleitung der gewünschten Nutzerdaten nach Maßgabe der Zweckbestimmung des Kunden erfolgen würde. Sie müssten neutral sein und den Nutzerinteressen dienen. Dabei dürften sie **keine Nutzerdaten monetarisieren**, müssten aber von Unternehmen, die diese Dienste anbieten, **Entgelte** für die Erbringung ihrer Dienste bei der **Einwilligungsverwaltung** erheben dürfen. Anderenfalls müsste Nutzer/innen oder der Staat für die Schaffung und den Betrieb der Dienste aufkommen. Nutzer/innen würden mit ihrer Hilfe die Kontrolle über ihre Daten zurückerlangen. Der Datenschutz wäre ebenso gesichert wie der Wettbewerb. Endlich könnten Nutzer damit auch den stetigen Cookie-Abfragen ein Ende setzen, die heute ohnehin kaum noch jemand versteht.

Der Veranschaulichung der Funktion von Diensten zur Einwilligungsverwaltung können folgende **Abbildungen** dienen:

[10] *Schwartmann/Weiß* (Hrsg.) Datenmanagement und Datentreuhandsysteme – Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digitalgipfels 2020, S. 15. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=2.

Abbildung 1: Wie erhebt der Dienst Einwilligungen und bietet dem Nutzer dann den Treuhänder an?

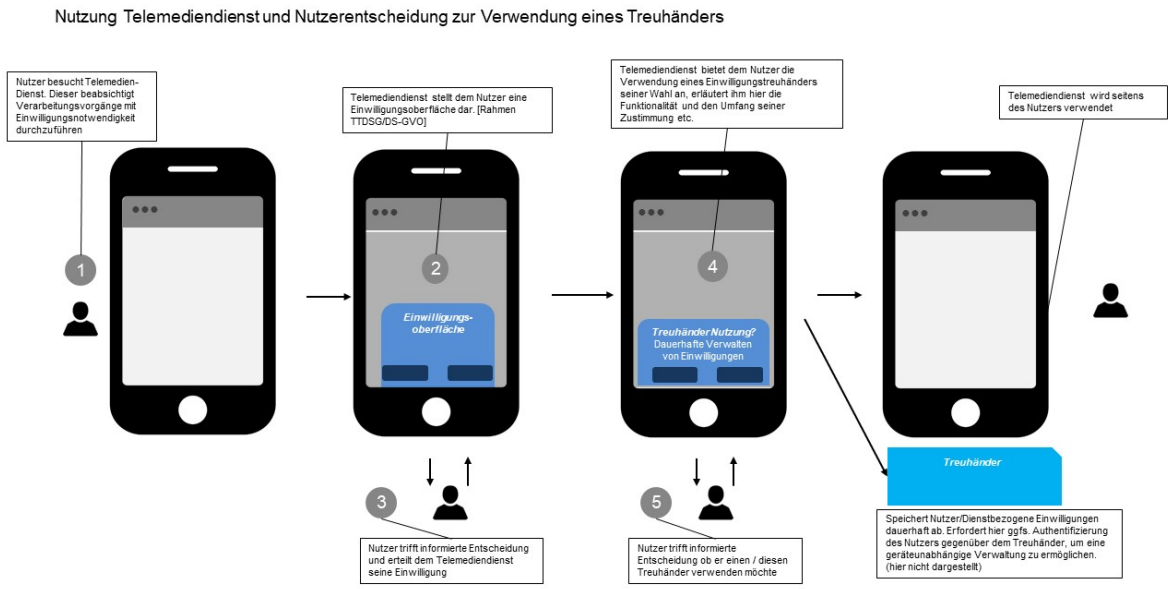
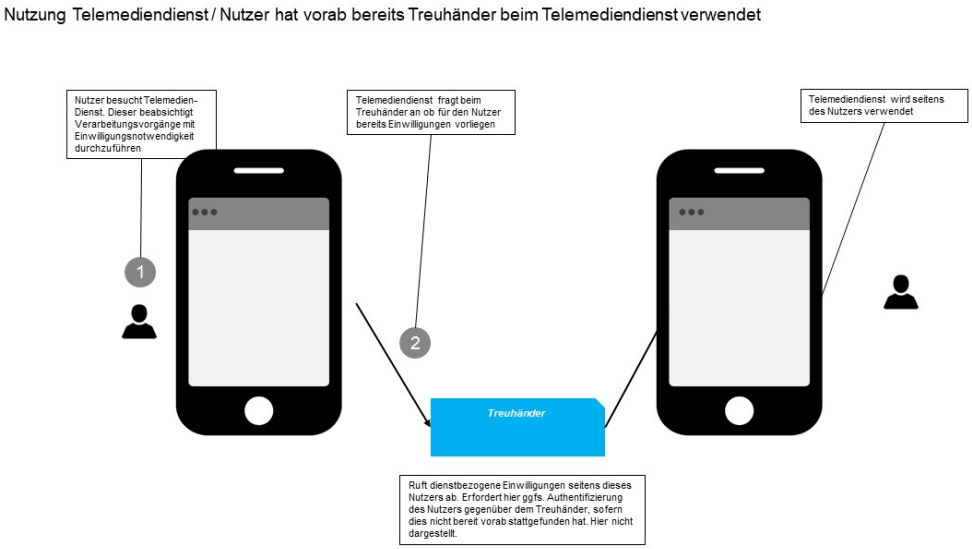


Abbildung 2: Wie ruft der Dienst bestehende Einwilligungen, ab und verhindert damit die wiederholende Anzeige von Dialogen?



d) Anforderungen an Dienste zur Einwilligungsverwaltung

Bei der Einführung einer Regelung zu PIMS sollten folgende Rahmenbedingungen beachtet werden:

- **Maßgeblichkeit des Willens der Nutzer/innen**

Nutzer/innen sollte über den Dienst zur Einwilligungsverwaltung (PIMS) nicht nur Zugriff und Speicherung von Informationen sondern auch in die anschließende Weiterverarbeitung personenbezogener Daten einwilligen können. Die Einwilligung oder deren Ablehnung ist für alle Akteure, also insbesondere Telemedienanbieter und Browseranbieter verbindlich.

- **Geschäftsmodell**

PIMS-Anbieter dürfen nicht an der Nutzung der verwalteten Daten verdienen, für ihre Dienste aber durchaus Entgelte erheben dürfen. Das muss gesetzlich klargestellt werden. Der frühere Gesetzesentwurf für einen § 3 TTDSG-E (Sommer 2020) eignete sich für diese Klarstellung nicht, da er selbst mittelbare wirtschaftliche Abhängigkeiten ausschloss.[11] Eine klarstellende Formulierung könnte lauten:

> *Dienste zur Einwilligungsverwaltung können unter der Voraussetzung anerkannt werden, dass sie kein wirtschaftliches Eigeninteresse an den im Auftrag der Endnutzer verwalteten Daten haben. Dem steht nicht entgegen, dass der Dienst für die Verwaltung der Daten ein Entgelt erhebt.*[12]

Eine geeignete Formulierung kann alternativ auch auf die aus datenschutzrechtlicher Sicht gebotene **besondere Zweckbindung** für die Verarbeitung von Daten aus PIMS abstellen. Anbieter von Diensten zur Einwilligungsverwaltung dürften danach die Informationen über die Einwilligungsentscheidungen der Nutzer für keine anderen Zwecke als die Einwilligungsverwaltung verwenden.[13]

Eine dies regelnde Norm kann wie folgt lauten:

> *Anbieter von Diensten zur Einwilligungsverwaltung dürfen die Informationen über die Einwilligungsentscheidungen der Nutzer für keine anderen Zwecke als die Einwilligungsverwaltung verwenden.*

- **Anerkennung der Dienste zur Einwilligungsverwaltung**

---

[11] Hierzu *Hofmann/Schwartmann/Weiß*, Kurzgutachten im Auftrag der European netID Foundation verpflichtende Einführung eines EU Single Sign-On, Januar 2021, S. 32 ff., abrufbar unter https://t1p.de/5o3u.

[12] *Hofmann/Schwartmann/Weiß*, Kurzgutachten im Auftrag der European netID Foundation verpflichtende Einführung eines EU Single Sign-On, Januar 2021, S. 32 ff., abrufbar unter https://t1p.de/5o3u.

[13] *Schwartmann/Hanloser/Weiß*, Kurzgutachten zu PIMS im TTDSG - Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, März 2021.

Entsprechende Angebote sollten nur von akkreditierten Datentreuhändern erbracht werden dürfen. Nicht akkreditierte transatlantische Angebote (GAFA) würden ihr Geschäft ansonsten ungestört weiter betreiben können, während rechtstreue europäische Dienste ihr Image ohne messbaren Nutzen durch eine freiwillige Akkreditierung lediglich symbolisch aufpolieren könnten.

Eine entsprechende Formulierung könnte lauten:

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

3. Geltung des Fernmeldegeheimnisses für die Privatnutzung gestattende Arbeitgeber (§ 3 TTDSG-E)

Ein wesentlicher Unterschied zwischen TTDSG Referenten- (TTDSG-RefE) und Regierungsentwurf (TTDSG-RegE) besteht darin, dass nach dem Referentenentwurf nur Anbieter öffentlicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze zur Wahrung des Fernmeldegeheimnisses verpflichtet sein sollten (§ 3 Abs. 2 TTDSG-RefE).

Damit wäre klar gewesen, dass **Arbeitgeber**, welche die private Nutzung der Telekommunikationssysteme durch Beschäftigte zulassen, **nicht erfasst** sind. Nach dem Regierungsentwurf sind nunmehr auch „Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten“ zur Wahrung des Fernmeldegeheimnisses verpflichtet (§ 3 Abs. 2 Nr. 2 TTDSG-RegE). Da für die Geschäftsmäßigkeit nicht die Gewinnerzielungsabsicht, sondern die Nachhaltigkeit des Angebots entscheidend ist, bliebe es also bei der schon lang andauernden Diskussion um die rechtlichen Konsequenzen der erlaubten Privatnutzung.

Insoweit sollte wieder zu der **Regelung im Referentenentwurf zurückgekehrt** werden. Hierfür spricht insbesondere Art. 3 der ePrivacy-Richtlinie. Danach gilt die Richtlinie lediglich für „die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft“. Die durch Art. 95 DS-GVO angeordnete Spezialität der ePrivacy-Richtlinie im Verhältnis zur allgemeineren DS-GVO kann jedoch nur so weit reichen, wie der Anwendungsbereich der ePrivacy-Richtlinie geht. Unternehmen, die ihren Arbeitnehmern die private Nutzung von E-Mail und Internet am Arbeitsplatz gestatten, unterfallen folglich nach den europarechtlichen Vorgaben dem allgemeinen Datenschutzrecht, also der DS-GVO.[14]

[14] *Koreng/Lachenmann/Bergt*, DatenschutzR-FormHdB, C. VII. 2.

Dies ist auch sachgerecht. Denn die betroffenen Kommunikationsmittel dienen im Ausgangspunkt eigenen Kommunikationszwecken des Arbeitgebers 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 ausgesetzt sieht. Der Arbeitgeber ist auch mit anderen Anbietern für geschlossene Benutzergruppen, z.B. Hotels oder Krankenhäusern, nicht vergleichbar, da er für seine eigenen unternehmerischen Zwecke ggf. auf den Zugriff auf Kommunikationsdaten angewiesen ist. Insofern bedarf es eines angemessenen Interessenausgleichs zwischen den unternehmerischen Zwecken des Arbeitgebers einerseits und den berechtigten Interessen der Beschäftigten andererseits.

Eine Einschränkung des Anwendungsbereichs des Fernmeldegeheimnisses ließe die betroffenen Arbeitnehmer schließlich keineswegs schutzlos. Denn Zugriffe des Arbeitgebers auf im Zusammenhang mit der Kommunikation angefallene Informationen hätten die Vorgaben der DS-GVO zu beachten. Die Verletzung dieser Bestimmungen kann mit erheblichen Bußgeldern belegt werden (Art. 83 DS-GVO). Die Einschränkung erscheint auch vor dem Hintergrund angemessen, dass in Zeiten von Mobilfunk, Smartphones und mobilem Internet kein Beschäftigter mehr auf die Nutzung betrieblicher Kommunikationsmittel für private Zwecke angewiesen ist.

Einschränkungen vom Anwendungsbereich des TTDSG sollten auch für Telemedienangebote des Arbeitgebers gelten. Eine vergleichbare Regelung, wie sie **heute § 11 TMG** enthält, fehlt und sollte ergänzt werden.

4. Gebot der anonymen und pseudonymen Nutzbarkeit von Telemedien (§ 19 Abs. 2 TTDSG-E)

Gemäß § 19 Abs. 2 TTDSG-E haben Anbieter von Telemedien die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer von Telemedien ist über diese Möglichkeit zu informieren. Insofern werden die bisherigen Regelungen aus § 13 Abs. 5 und 6 TMG übernommen. Diese Anforderungen gelten allerdings zu Recht als technisch und rechtlich überholt[15] und in der Praxis nahezu nicht umsetzbar. Eine **anonyme Nutzung** ist vielfach bereits technisch **unmöglich**, da bei der elektronischen Kommunikation eine Vielzahl von (Geräte)-Kennungen verwendet werden, um die Diensterbringung zu ermöglichen. Jedenfalls das **Gebot der anonymen Nutzbarkeit von Telemedien sollte** deshalb **entfallen**. Ob eine pseudonyme Nutzung zumutbar ist, bestimmt sich in erster Linie nach dem Geschäftsmodell des Anbieters von Telemedien.[16]

[15] Vgl. *Schwartmann/Benedikt/Reif*, MMR 2021, 99 (100).
[16] *Roßnagel*, Beck'scher Komm. Telemediendienste, 1. Aufl., TMG § 13 Rn. 130.