STELLUNGNAHME

Stellungnahme des Bundesverbands Digitale Wirtschaft e.V. zum Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien sowie zur Änderung des Telemediengesetzes

22.01.2021

Vorbemerkungen

Der **Bundesverband Digitale Wirtschaft (BVDW) e.V**. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld.

Ansprechpartner:

Christian Dürschmied
Referent Datenschutz, Data Economy
T: +49 30 2062186-23
duerschmied@bvdw.org

Zusammenfassung

Der BVDW kann den Referentenentwurf für ein Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) in der vorliegenden Fassung **nicht** unterstützen.

Im Einzelnen:

1. Der BVDW begrüßt, dass sich § 22 TTDSG am Wortlaut von Artikel 5 Abs. 3 der E-Privacy-Richtlinie orientiert.

   Wir haben jedoch auch Bedenken, da sehr praxisrelevante Anwendungsbereiche nicht berücksichtigt werden.

   Identifizierung, Integritäts- und Sicherheitsüberprüfungen, Werbeblocker sowie Leistungs-, Nutzungs- und Reichweitenmessungen durch Telemedienanbieter und Drittanbieter, insbesondere auch zu Abrechnungszwecken im Falle von Online-Werbung, sind für das

ordnungsgemäße Funktionieren einer Webseite oder die Anwendung und Bereitstellung eines Dienstes unbedingt erforderlich.

Leistungs-, Nutzungs- oder Reichweitenmessungen sind beispielsweise zum Zwecke der Erkennung von Navigations- oder Darstellungsproblemen, der ordnungsgemäßen Provisionierung und Wirkung von Werbung, der Optimierung von technischer Leistung, der Analyse besuchter Inhalte, der unabhängigen Feststellung der „Online-Auflage" bzw. Mediennutzung durch reine Zählung (vergleichbar einem Handzähler / Personenzähler) oder des Zugriffs auf eine Inhaltsprobe unbedingt erforderlich, um die vom Nutzer ausdrücklich gewünschten Dienste zur Verfügung stellen zu können.

Im Bereich des automatisierten und vernetzen Fahrens 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). Auch wenn andere Telemedienanbieter oder die von einem Telemedienanbieter beauftragten Dritten Maßnahmen ergreifen, um den bereitgestellten Dienst abzusichern, sollte daher keine Einwilligungspflicht bestehen. Andere Telemedienanbieter, wie etwa ein Nachrichtenportal, sollten auf eigene oder durch Dritte bereitgestellte Sicherheitstechnologien oder Sicherheitsdienste zurückgreifen können, um zum Beispiel die Informationssicherheit, ein Sicherheitsmonitoring, eine Betrugsprävention, einen unberechtigten Zugang oder Sicherheitsangriffe sowie eine effiziente und sichere Auslieferung von Inhalten ermöglichen zu können. Der in der vorliegenden Gesetzesbegründung bereits klar zum Ausdruck kommende Gedanke, dass sicherheitsspezifische Fragestellungen generell explizit erfasst sein sollen, muss im Interesse der Anbieter und Nutzer nicht nur für bestimmte Industriezweige gelten, sondern für den Bereich der Telemedien (Webseiten, Apps) insgesamt. Wir schlagen vor, den sachlichen Erwägungsgrund zu verallgemeinern und die Gesetzesbegründung wie folgt zu fassen:

„.....Dies gilt im Bereich der Telemedien ebenso für das Speichern und Auslesen von Informationen auf Endeinrichtungen aus Sicherheitsgründen, aus Gründen der Informationssicherheit und der Betrugsbekämpfung".

Die Speicherung von Informationen in der Endrichtung des Endnutzers oder der Zugriff auf diese Informationen kann auch dann unbedingt erforderlich sein, um dem Nutzer den auf vertraglicher Basis ausdrücklich gewünschten Telemediendienst zur Verfügung zu stellen. Auch diese Möglichkeit ist für die Praxis nach wie vor und auch in Zukunft – wie die im Referentenentwurf angeführten Beispiele zu innovativen Zukunftsfeldern zeigen – von hoher Relevanz, insbesondere wenn eine Interaktionsmöglichkeit bzw. ein Kontakt mit dem Nutzer nicht möglich ist oder aber gewünschte Funktionalitäten gewährleistet werden müssen, z. B. bei IOT-Geräten.

Wir regen daher an, die Richtlinienkonformität klarzustellen, beispielsweise indem der Referentenentwurf in der Begründung noch weitere praxisrelevante Beispiele anführt, die im Einklang mit Artikel 5 Abs. 3 der E-Privacy-Richtlinie von den Ausnahmeregelungen umfasst sind.

2. Ein einfacher und handhabungsfreundlicher Datenschutz ist das Ziel. Dabei können Instrumente des Selbstdatenschutzes die Datensouveränität des Nutzers stärken, die Ausübung von Rechten ermöglichen und die Verwaltung von Digitalen bzw. Online-Identitäten erleichtern.

Ein einfacher und handhabungsfreundlicher Datenschutz ermöglicht Unternehmen der Digitalen Wirtschaft eine datenschutzkonforme Ausgestaltung ihrer Prozesse und verringert die Aufwände für Unternehmen erheblich,[1] etwa durch Instrumente wie zum Beispiel Personal Information Management Systeme, die sowohl auf europäischer Ebene[2] als auch durch die Bundesregierung[3] unterstützt werden.

Dazu wurde angeregt, eine rechtliche Grundlage für die Anerkennung und die Tätigkeit entsprechender Systeme zu schaffen. Die Ausgestaltung könnte durch Qualitätsstandards und die Einführung von Zertifizierungs- und Überwachungssystemen weiter vorangebracht werden. Die Festlegung einer Treuepflicht gegenüber Nutzern, der Ausschluss Beteiligter mit

[1] s. auch Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020 zu Datenmanagement- und Datentreuhandsystemen, abrufbar über die Webseite des BMWi: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und datentreuhand-systeme.pdf?__blob=publicationFile&v=2).

[2] vgl. etwa EDPS Opinion on Personal Information Management Systems: "Towards more user empowerment in managing and processing personal data", https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en

[3] Koalitionsvertrag zwischen CDU, CSU und SPD, April 2018, S. 47, www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906

gegenläufigen Interessen und Kontrollmöglichkeiten können zu einem „Interessenwalter“ der Nutzer führen, der einem Zulassungsverfahren und einer Aufsicht unterliegt und seinen Sitz in der Europäischen Union hat. Regelungen zur IT-Sicherheit können das Vertrauen stärken. Maschinen-interpretierbare Formate und Kommunikationsprotokolle können Standardisierungen erleichtern. Mit Blick auf die Zukunft ergeben sich Spielräume, um die Daten für die europäische Datenwirtschaft datenschutzkonform freizusetzen. Über Datenzugangsmöglichkeiten – etwa durch Datenfreigabe des Nutzers – können beispielsweise Forschungsvorhaben unterstützt werden, weshalb Regelungen für Datenschutzmanagementsysteme bzw. Personal Information Management Systeme (sog. PIMS) angeregt werden.[4]

Ein Rückgriff auf derartige Systeme sollte allerdings auch den Telemedienanbietern überlassen bleiben und freiwillig sein. Die Einwilligung eines Nutzers sollte auch den Einstellungen dieser Systeme vorgehen.

Mit Blick auf die Zukunft werden dadurch für Nutzer, die Gesellschaft und die Wirtschaft letztlich Datensouveränitäts- und Datenidentitätsmanagementsysteme sowie Datenzugangs- bzw. Datenteilungssysteme geschaffen.

Derzeit ist nicht absehbar, wann und wie der Data Governance Act final gestaltet sein wird. Wenn Deutschland durch gesetzliche Regelungen die Bedeutung dieser Thematik unterstreicht, können diese für die weiteren Diskussionen auf europäischer Ebene zu den zentralen Rahmenbedingungen der Digitalisierung führen, was sich aufgrund nationaler Vorstöße bereits gezeigt hat.

3. Wenn unmittelbar erteilte Einwilligungen des Nutzers gegenüber dem Telemedienanbieter beispielsweise gegenüber Betriebssystemen, Mobile Operating Systems, Browsereinstellungen, Einstellungen bei Personal Information Management Systemen oder gegenüber anderen technischen Voreinstellungen grundsätzlichen Vorrang haben, wird das Recht auf Schutz personenbezogener Daten und der Schutz der Privatsphäre nutzerzentriert und damit auch tatsächlich verbraucherfreundlich ausgestaltet. Gleichzeitig werden Missbrauchsmöglichkeiten und Beeinträchtigungen

[4] Gutachten der Datenethikkommission der Bundesregierung, S. 133 ff.

des Wettbewerbs unterbunden. Denn allein die Entscheidung des Nutzers ist maßgeblich und muss vom verantwortlichen Diensteanbieter umgesetzt werden. Dies kann beispielsweise durch die Aufnahme einer weit gefassten Befolgungspflicht, die derzeit diskutiert wird, gewährleistet werden.

Der BVDW spricht sich allerdings zudem dafür aus, dass die damit in Zusammenhang stehenden Sach- und Rechtsfragen zur Validierung und Standardisierung der Einwilligungskommunikation, beispielsweise durch Instrumente wie dem Transparency and Consent Framework des IAB Europe TCF, gesetzlich verankert werden. Hierdurch sollten auch Fragen der datenschutzrechtlichen Verantwortlichkeit konkretisiert werden.

4. Wir möchten schließlich noch auf **folgende Punkte** hinweisen:

- Das Verhältnis von TTDSG und DSGVO ist in gewisser Hinsicht erkennbar, gleichwohl regen wir an, dieses – auch mit Blick auf Art. 95 DSGVO – klarzustellen.

- Abweichend vom generell einschlägigen Herkunftslandsprinzip wird in § 1 TTDSG ein Marktortprinzip beschrieben, das auch für "Angebote" in Deutschland gelten soll. Damit wird der Anwendungsbereich gleichzeitig auch auf Unternehmen in Drittstaaten außerhalb der EU erstreckt, die in Deutschland Dienstleistungen erbringen. Es wird allerdings nicht klargestellt, wie die Einhaltung der Regelungen gegenüber Unternehmen aus Drittstaaten sichergestellt werden soll. Auch soll das "Mitwirken" zur Eröffnung des Anwendungsbereichs führen. Inwieweit hier beispielsweise technische Dienstleister, die Auftragsarbeiten für Anbieter in Deutschland durchführen, erfasst sein können, ist nicht klar. Auch diese sollen hiervon wohl nicht umfasst sein.

- Das Wort "erforderlich" in § 2 TTDSG schränkt die Definition des Verkehrsdatums, welches unter die Regelungen des TTDSG fallen sollen, ein. Da eine Reihe von Daten, die nicht unbedingt erforderlich sind, davon nicht erfasst sind, wäre eine Klarstellung hilfreich.

- Auch eine Klarstellung dazu, worauf sich die Beschreibungen in § 6 TTDSG konkret beziehen und worauf sich der Anwendungsbereich erstreckt, wäre hilfreich. So stellt sich beispielsweise die

Frage, ob technisch notwendige Zwischenspeicherungen (wie das sog. Caching von Daten) von dieser Regelung umfasst sind.

- Die Zuständigkeit des BfDI für Bußgeldverfahren im Zusammenhang mit § 22 TTDSG erscheint fraglich. Eine zentrale Zuständigkeit des BfDI und nicht eine Zuständigkeit der Landesdatenschutzaufsichtsbehörden soll sich wohl aus dem Gesetzesentwurf ergeben.

- Wir möchten auch in diesem Zusammenhang noch einmal darauf hinweisen, dass heutige Webangebote wie kostenfreie journalistische Inhalte, kommunikations- und andere Spezialdienste Nutzern nur deshalb kostenfrei angeboten werden können, weil Werbetreibende, Agenturen, Vermarkter oder Adtech-Unternehmen die Angebote – wie beim privaten und öffentlich-rechtlichen Fernsehen – durch einen Beitrag unmittelbar oder mittelbar finanzieren und dadurch einen wertvollen gesellschaftlichen Beitrag für die Meinungsvielfalt leisten. Um der Bedeutung des Rechts auf freie Meinungsäußerung Rechnung zu tragen, müssen sich Medienunternehmen, die sich auf diese Freiheit beziehen, finanzieren können. Die Möglichkeit zur Finanzierung ist unverzichtbare Voraussetzung für den Fortbestand dieser Meinungsvielfalt und für den Fortbestand eines professionellen Journalismus (vgl. etwa EuGH, Urt. v. 16. 12. 2008 – C-73/07). Im Einklang mit europäischen Entwicklungen käme die Finanzierung von Medienunternehmen, insbesondere journalistische Tätigkeiten, auch ohne rechtliche Risiken in Betracht („Medienprivileg“).

- 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.

  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 die Anbieter von Kommunikationsdiensten berechtigt sein sollten, ein kostenorientiertes Entgelt zu erheben.

Unter Berücksichtigung der politischen Ziele zur Datenökonomie und der wirtschaftlichen Aspekte der betroffenen Unternehmen, regen wir an, diese Regelungen entsprechend zu überdenken.

- Die weitreichende Thematik zur Identifizierungspflicht bei Telemedien darf nicht über ein TTDSG ohne Weiteres „mitgeregelt" werden. Die Regelung ist nicht nachvollziehbar. In diesem Zusammenhang stellen sich daher zahlreiche Fragen. So fragen wir uns beispielsweise, wozu die Regelung benötigt wird und weshalb im Rahmen des TTDSG ein Regelungsbedarf gesehen wird. Weiter stellt sich zum Beispiel die Frage, wie die damit verbundenen grundrechtlichen Fragestellungen beantwortet wurden.

5. Die Ausführungen sind nicht abschließend. Weitere Ausführungen werden ausdrücklich vorbehalten.