

# DATENSCHUTZ UND PRIVAT- SPHÄRE BEI TELEKOMMUNIKATI- ONSDIENSTEN UND TELEMEDIEN SICHERSTELLEN

Stellungnahme des Verbraucherzentrale Bundesverbands  
zum Referentenentwurf des Bundesministeriums für Wirt-  
schaft und Energie für ein Telekommunikations-Telemedien-  
Datenschutzgesetz (TTDSG-E)

21. Januar 2021

## Impressum

Verbraucherzentrale  
Bundesverband e.V.

Team  
Digitales und Medien

Rudi-Dutschke-Straße 17  
10969 Berlin

[digitales@vzbv.de](mailto:digitales@vzbv.de)

# INHALT

<b>I. ZUSAMMENFASSUNG</b>	<b>3</b>
<b>II. EINLEITUNG</b>	<b>4</b>
<b>III. POSITIONEN IM EINZELNEN</b>	<b>4</b>
1. Zu den Fragestellungen des BMWi.....	4
1.1 Regelungen zu Datenmanagementsystemen und „Personal Information Management-services“ (PIMS) .....	4
1.2 Regelungen zu Browsereinstellungen.....	5
2. Zu den Regelungen des TTDSG-E .....	7
2.1 § 22 - Einwilligungen bei Endeinrichtungen .....	7
2.2 § 19 - Technische und organisatorische Vorkehrungen .....	7

# I. ZUSAMMENFASSUNG

Am 12. Januar 2020 veröffentlichte das Bundesministerium für Wirtschaft und Energie (BMWi) einen Referentenentwurf für ein Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG-E).<sup>1</sup> Darüber hinaus bittet das BMWi um Stellungnahmen zu weiteren konkreten Regelungsfragen, die derzeit nicht im Referentenentwurf enthalten sind.<sup>2</sup>

Der Verbraucherzentrale Bundesverband (vzbv) begrüßt den Entwurf sowie die weiterführenden Fragen des BMWi, sieht aber noch zusätzlichen Bedarf, Verbraucherinnen und Verbraucher<sup>3</sup> besser zu schützen. Zusammenfassend nimmt der vzbv dazu wie folgt Stellung:

- ❖ Eine Regulierung von neuen Datenmittlern sollte nicht im Rahmen des TTDSG, sondern auf europäischer Ebene als horizontale Vorschrift erfolgen.
- ❖ Der Vorschlag des BMWi für eine Regelung zu Browsereinstellungen greift deutlich zu kurz. Software, die den Abruf von Informationen aus dem Internet oder eine elektronische Kommunikation erlaubt, sollte stets datenschutzfreundlich voreingestellt sein müssen. Darüber hinaus sollte ein granulares Whitelisting sichergestellt werden, sodass eine Einwilligung, die ein Verbraucher dem Anbieter eines Dienstes erteilt, auch technisch durch die Software übernommen werden muss. Ein solches Whitelisting würde dem Ansinnen des BMWi entsprechen.  
In jedem Fall sollte die Bundesregierung weiterhin anstreben, entsprechende Regelungen auf europäischer Ebene in der kommenden ePrivacy-Verordnung zu verankern.
- ❖ Der vzbv begrüßt, dass das BMWi eine Regelung eng am Wortlaut der Vorgaben der ePrivacy-Richtlinie vorschlägt, nach der das Speichern und Auslesen von Informationen auf den Endeinrichtungen der Verbraucher grundsätzlich nur nach einer zuvor erteilten, informierten Einwilligung zulässig ist.
- ❖ Der vzbv unterstützt, die bestehenden Regelungen des § 13 Abs. 6 TMG in das TTDSG zu übernehmen, nach denen Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonymen zu ermöglichen haben. Gesetzliche Vorgaben für Diensteanbieter zur Identifizierung zwecks Verifikation der Nutzer lehnt der vzbv ab.

---

<sup>1</sup> Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien sowie zur Änderung des Telemediengesetzes vom 12.01.2021; URL: <https://www.bmwi.de/Redaktion/DE/Downloads/P-R/referentenentwurf-zum-gesetz-zur-regelung-des-datenschutzes-und-des-schutzes-privatsphaere.pdf> [Zugriff: 12.01.2021]. Alle Verweise auf Paragraphen und Begründungen ohne Gesetzesangaben beziehen sich auf das TTDSG-E.

<sup>2</sup> Bundesministerium für Wirtschaft und Energie: Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (2021); URL: <https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/gesetz-zur-regelung-des-datenschutzes-und-des-schutzes-privatsphaere.html> [Zugriff: 12.01.2021].

<sup>3</sup> Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Mehrfachbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

## II. EINLEITUNG

Mit dem TTDSG sollen die Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) zusammengeführt und an die Datenschutz-Grundverordnung (DSGVO) angepasst werden.

Der vzbv unterstützt dieses Ziel. Das Nebeneinander der Regelungen, sowie die zum Teil nicht erfolgte Umsetzung der ePrivacy-Richtlinie in nationales Recht, haben in den vergangenen Jahren zu einer erheblichen Rechtsunsicherheit bei Verbrauchern sowie Anbietern von Telemedien und Telekommunikationsdiensten geführt. Insbesondere begrüßt der vzbv, dass sich die nun vorgeschlagenen Regelungen zum Speichern und Auslesen von Informationen auf den Endgeräten der Nutzer eng am Wortlaut der Vorgaben der ePrivacy-Richtlinie orientieren.

Der vzbv bedankt sich beim BMWi für die Gelegenheit, zu diesem Entwurf sowie zu weiteren Regelungsfragen Stellung nehmen zu können. Jedoch bedauert der vzbv die äußerst kurze Kommentierungsfrist von nur wenigen Tagen, sodass im Rahmen dieser Stellungnahme lediglich auf die drängendsten Punkte eingegangen werden kann. Der vzbv behält sich vor, darüber hinaus gehende Aspekte im weiteren Verlauf des Gesetzgebungsverfahrens vorzubringen.

## III. POSITIONEN IM EINZELNEN

### 1. ZU DEN FRAGESTELLUNGEN DES BMWI

#### 1.1 Regelungen zu Datenmanagementsystemen und „Personal Information Management Services“ (PIMS)

Grundsätzlich begrüßt der vzbv das Ansinnen des BMWi, neuen Datenintermediären einen rechtlichen Rahmen zu geben, um den Austausch von Daten zu erleichtern, ohne dabei Abstriche beim Schutz der personenbezogenen Daten der Betroffenen machen zu müssen.<sup>4</sup>

Allerdings bezweifelt der vzbv, dass das TTDSG der geeignete Ort für eine solche Regelung wäre. Vielmehr sollten entsprechende Vorgaben auf EU-Ebene verankert werden. So hätte eine Regelung im TTDSG sowohl hinsichtlich der erfassten Dienste (lediglich elektronische Kommunikationsdienste sowie Telemedien), als auch hinsichtlich der durch die Betroffenen wahrnehmbaren Rechte (Erteilung von Einwilligungen zu eng begrenzten Zwecken) einen deutlich zu engen Anwendungsbereich. Weitere Rechte, die den Betroffenen entsprechend der DSGVO zustehen (wie etwa das Recht auf Auskunft) oder beispielsweise die Möglichkeit, Datenmittler als Schnittstelle zwischen Verbrauchern und Forschungseinrichtungen zu etablieren, könnten über das TTDSG nicht abgedeckt werden.

---

<sup>4</sup> Vgl. Verbraucherzentrale Bundesverband: Neue Datenintermediäre - Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder (2020); URL: [https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15\\_vzbv-positionspapier\\_datenintermediaere.pdf](https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf) [Zugriff: 13.01.2021].

Da die Europäische Kommission mit dem Daten-Governance-Gesetz bereits einen entsprechenden Vorschlag<sup>5</sup> zur Diskussion gestellt hat<sup>6</sup> und das deutsche TTDSG nur einen sektoralen Ansatz verfolgt, spricht sich der vzbv für eine europäische Regelung aus. Der vzbv hat diese Position bereits im Rahmen der Datenethikkommission vertreten.

Eine Regulierung von neuen Datenmittlern sollte nicht im Rahmen des TTDSG, sondern auf europäischer Ebene als horizontale Vorschrift erfolgen.

## 1.2 Regelungen zu Browsereinstellungen

Das BMWi spricht sich für die Einführung einer Regelung zu Browsereinstellungen im TTDSG aus, die verhindern soll, dass Browser herstellereitig so eingestellt werden, dass der Zugriff auf die Informationen in Endeinrichtungen verhindert wird, auch wenn der Endnutzer eingewilligt hat.

Auch der vzbv fordert Regelungen für technische Ansätze, mit deren Hilfe Endnutzer die Speicherung von Informationen in ihren Endeinrichtungen oder den Zugriff auf solche Informationen zentral steuern können. Dazu gehört, dass ein Whitelisting möglichst einfach durch die entsprechende Software erfolgen muss, wenn dem Anbieter eines Dienstes eine Einwilligung zur Speicherung von Informationen auf dem Endgerät erteilt wurde. Dies würde dem Ansinnen des BMWi entsprechen, dass eine Einwilligung, die ein Verbraucher dem Betreiber einer Webseite erteilt, auch technisch durch die Webbrowser übernommen werden muss.

Jedoch greift der Vorschlag des BMWi deutlich zu kurz. Um den Schutz personenbezogener Daten sowie den Schutz der Privatsphäre der Verbraucher zu gewährleisten, bedarf es dringend einer Regelung, dass die Gestaltung von Software, die den Abruf von Informationen aus dem Internet oder eine elektronische Kommunikation erlaubt, stets dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen folgen muss. Lediglich Informationen, für die entsprechend der ePrivacy-Richtlinie keine Einwilligung erforderlich ist, sollten per Voreinstellung gespeichert und abgerufen werden dürfen. Das Flash Eurobarometer 443 der EU-Kommission zeigt eindeutig, dass sich die Verbraucher datenschutzfreundliche Voreinstellungen wünschen. In dieser Studie hatten sich 90 Prozent der deutschen Internetnutzer für solche Voreinstellungen in ihren Webbrowsern ausgesprochen.<sup>7</sup> Gleichzeitig zeigt die Studie auch, dass besonders ältere Menschen, Menschen mit niedriger Bildung sowie Menschen, die das Internet wenig verwenden, seltener Änderungen in den Datenschutzeinstellungen ihrer Software vornehmen.<sup>8</sup> Datenschutzfreundliche Voreinstellungen schützen also in erster Linie diese besonders vulnerablen Verbrauchergruppen.

---

<sup>5</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und Rates über europäische Daten-Governance (Daten-Governance-Gesetz).

<sup>6</sup> Siehe auch Stellungnahme des Verbraucherzentrale Bundesverbands zum Vorschlag der EU-Kommission für eine Verordnung über europäische Daten-Governance (2021); URL: [https://www.vzbv.de/sites/default/files/downloads/2021/01/13/21-01-12\\_vzbv-stellungnahme\\_data-governance-act.pdf](https://www.vzbv.de/sites/default/files/downloads/2021/01/13/21-01-12_vzbv-stellungnahme_data-governance-act.pdf) [Zugriff: 15.01.2021].

<sup>7</sup> Europäische Kommission: Flash Eurobarometer 443 (2016); S. 46; URL: [https://data.europa.eu/euodp/en/data/dataset/S2124\\_443\\_ENG](https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG) [Zugriff 14.01.2021].

<sup>8</sup> Ebenda; S. 37.

Dabei darf eine solche Regelung nicht auf Webbrowser begrenzt sein, sondern muss jegliche Software umfassen, mit der Informationen aus dem Internet abgerufen werden können oder die eine elektronische Kommunikation erlaubt. Dazu gehören neben Webbrowsern auch andere (mobile) Applikationen sowie die Betriebssysteme der Endgeräte. Gleichmaßen darf eine solche Regelung nicht alleine auf eine Technologie (zum Beispiel http-Cookies) ausgerichtet sein, sondern muss technikneutral formuliert werden, um auch andere Informationen wie weitere Cookie-, Fingerprinting- und Telemetrie-Technologien einzuschließen.

Darüber hinaus muss klargestellt sein, dass ein Whitelisting – wie auch die Einwilligung als solche – granular erfolgen muss. Dies wird durch die gängigen Browser bisher technisch nicht abgebildet. Zum einen unterscheiden diese bisher meist lediglich zwischen http-Cookies, die von Erstanbietern oder Drittanbietern gesetzt werden. Dies entspricht jedoch nicht der Unterscheidung zwischen Informationen, für die entsprechend der e-Privacy-Richtlinie eine Einwilligung erforderlich ist und Informationen, bei denen dies nicht der Fall ist. In der Praxis erfolgt jedoch beispielsweise das Tracking zu Werbezwecken zum Teil auch über Erstanbieter-Cookies.<sup>9</sup> Zum anderen ist ein Whitelisting durch die Webbrowser bisher üblicherweise lediglich auf Domain-Ebene möglich. Dies bedeutet, dass Nutzer derzeit nicht selektiv auswählen können, ob sie beispielsweise Cookies zu Zwecken der Reichweitenmessung durch Drittanbieter akzeptieren, aber Cookies zu Werbezwecken ablehnen möchten.

In jedem Fall wäre eine diesen Maßgaben entsprechende nationale Regelung aus Sicht des vzbv nicht die beste Lösung. Vielmehr wäre die kommende ePrivacy-Verordnung der richtige Ort, solche Vorgaben zu verankern. Besonders das Europäische Parlament hat hierfür gute Vorschläge gemacht,<sup>10</sup> denen der Rat der Europäischen Union aus Sicht des vzbv folgen sollte. Der vzbv bedauert daher sehr, dass der entsprechende Regelungsvorschlag der EU-Kommission im Rahmen der Verhandlungen im EU-Rat ersatzlos gestrichen wurde. Die Bundesregierung sollte sich daher auch weiterhin für dessen Wiederaufnahme einsetzen.

Software, die den Abruf von Informationen aus dem Internet oder eine elektronische Kommunikation erlaubt, sollte stets datenschutzfreundlich voreingestellt sein müssen. Darüber hinaus sollte ein granulares Whitelisting sichergestellt werden, sodass eine Einwilligung, die ein Verbraucher dem Anbieter eines Dienstes erteilt, auch technisch durch die Software übernommen werden muss.

Die Bundesregierung sollte weiterhin anstreben, entsprechende Regelungen auf europäischer Ebene in der kommenden ePrivacy-Verordnung zu verankern.

<sup>9</sup> Vgl. Tremmel, Moritz: Facebook wechselt zu First-Party-Cookie. in: Golem.de (2018); URL: <https://www.golem.de/news/tracking-facebook-wechselt-zu-first-party-cookie-1810-136996.html> [Zugriff 14.01.2021].

<sup>10</sup> Siehe Entwurf einer legislativen Entschließung des Europäischen Parlaments vom 23.10.2017, A8-0324/2017

## 2. ZU DEN REGELUNGEN DES TTDSG-E

### 2.1 § 22 - Einwilligungen bei Endeinrichtungen

Der vzbv begrüßt, dass sich das BMWi dazu entschlossen hat, die ePrivacy-Richtlinie eng am Wortlaut umzusetzen. Positiv hervorzuheben ist insbesondere, dass nicht erneut der Versuch unternommen wird, über eine nationale Regelung neue Rechtsgrundlagen zum Speichern und Auslesen von Informationen auf den Endgeräten der Nutzer zu schaffen, die in der ePrivacy-Richtlinie nicht vorgesehen sind.

Denn nach Einschätzung des vzbv öffnen die ePrivacy-Richtlinie und die DSGVO keine Spielräume für weiterführende Regelungen. So enthält die ePrivacy-Richtlinie eine abschließende Auflistung, unter welchen Umständen das Speichern und Auslesen von Informationen auf den Endeinrichtungen der Nutzer auch ohne eine vorherige, informierte Einwilligung möglich ist.<sup>11</sup> Auch hinsichtlich der Anforderungen der Wirksamkeit einer Einwilligung der ePrivacy-Richtlinie sind die Anforderungen DSGVO maßgebend, wie unter anderem der Europäische Gerichtshof in der Rechtssache C-673/17 (Planet49) dargelegt hat.

Der vzbv begrüßt, dass das BMWi eine Regelung eng am Wortlaut der Vorgaben der ePrivacy-Richtlinie vorschlägt, nach der das Speichern und Auslesen von Informationen auf den Endeinrichtungen der Verbraucher grundsätzlich nur nach einer zuvor erteilten, informierten Einwilligung zulässig ist.

### 2.2 § 19 - Technische und organisatorische Vorkehrungen

Entsprechend der bestehenden Regelungen des § 13 Abs. 6 TMG – die nicht durch die DSGVO verdrängt werden<sup>12</sup> – haben Diensteanbieter, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonymen zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Um den Nutzern auch weiterhin die Möglichkeit zu geben, die Preisgabe ihrer persönlichen Daten gegenüber den Diensteanbietern zu vermeiden beziehungsweise zu minimieren, unterstützt der vzbv, die entsprechenden Vorschriften in das TTDSG zu übernehmen.

Das BMWi hat in diesem Kontext außerdem einen Vorschlag des Bundesministeriums des Inneren und der Innenministerkonferenz des Bundes und der Länder zur Diskussion gestellt, der gesetzliche Vorgaben zur Identifizierung zwecks Verifikation der Nutzer fordert.<sup>13</sup> Solche Vorgaben lehnt der vzbv jedoch ab. Nach der Rechtsprechung des Bundesverfassungsgerichts und des Bundesgerichtshofs ist die anonyme Nutzung dem Internet immanent. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde die Gefahr begründen, dass der Einzelne aus Furcht vor Repressa-

---

<sup>11</sup> Vgl. Artikel-29-Datenschutzgruppe: Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht. WP 194 (2012); URL: [https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe\\_EDSA/Stellungnahmen/WP194\\_Opinion42012CookieConsentExemption.pdf](https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP194_Opinion42012CookieConsentExemption.pdf) [Zugriff 14.01.2021].

<sup>12</sup> Vgl. OLG München, Endurteil vom 08.12.2020 - 18 U 5493/19 Pre, Rn. 65.

<sup>13</sup> Beschlussniederschrift der Frühjahrs-IMK. TOP 24 (2020); URL: [https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2020-06-17\\_19/beschluesse.pdf](https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2020-06-17_19/beschluesse.pdf) [Zugriff: 12.01.2021].

lien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern.<sup>14</sup> Vergleichbare Abschreckungseffekte sind auch zu befürchten, wenn sich die Nutzer alleine gegenüber den Diensteanbietern identifizieren müssen.

Darüber hinaus würde eine solche Verpflichtung neue Gefahren hinsichtlich des Datenschutzes und der Datensicherheit hervorrufen. So würde eine entsprechende Identifizierung den Diensteanbietern die Bildung und Verknüpfung von Profilen erleichtern, die wiederum zur (politischen) Manipulation der Nutzer verwendet werden könnten. Auch würde eine entsprechende Datensammlung weitere Begehrlichkeiten bei Strafverfolgungsbehörden wecken. Dies würde auf der einen Seite ein Risiko für die Rechte und Freiheiten der Verbraucher darstellen. Auf der anderen Seite könnten viele Nutzer davon abgeschreckt werden, sich überhaupt bei den jeweiligen Diensten anzumelden, die heutzutage ein wichtiges Medium zur politischen und gesellschaftlichen Meinungsbildung darstellen.

Der vzbv unterstützt, die bestehenden Regelungen des § 13 Abs. 6 TMG in das TTDSG zu übernehmen. Gesetzliche Vorgaben zur Identifizierung zwecks Verifikation der Nutzer lehnt der vzbv ab.

---

<sup>14</sup> Vgl. BGH, Urteil vom 23.06.2009 - VI ZR 196/08, BGHZ 181, 328, juris Rn. 38.