EPRIVACY-VERORDNUNG

Kernpositionen des Verbraucherzentrale Bundesverbands (vzbv) anlässlich der anstehenden Trilog-Verhandlungen (Stand: 06. Mai 2021)

KERNPOSITIONEN

- Der Europäische Gesetzgeber muss den Schutz persönlicher Daten und die Vertraulichkeit in der elektronischen Kommunikation wieder in den Vordergrund stellen. Ein Zurück hinter das Schutzniveau der bisherigen ePrivacy-Richtlinie ist nur in eng begrenzten Fällen unter strengen Voraussetzungen akzeptabel.
- Der Schutz der Verbraucherinnen und Verbraucher[1] kann nur gewährleistet werden, wenn die Verarbeitung elektronischer Kommunikationsdaten und der Zugriff auf Informationen auf den Endgeräten der Nutzer („Tracking“) ausschließlich zu gesetzlich festgelegten Zwecken unter strikten Bedingungen oder auf Basis der Einwilligung erfolgen darf.
- Eine Weiterverarbeitung von elektronischen Kommunikationsmetadaten für „kompatible Zwecke“ ist in diesem besonders sensiblen Bereich nicht akzeptabel und nicht mit der Rechtsprechung des Europäischen Gerichtshofs vereinbar. Daher lehnt der vzbv entsprechende Vorschläge vehement ab.
- Das Speichern von Informationen auf den Endgeräten der Nutzer beziehungsweise der Abruf solcher Informationen darf nicht als erforderlich für den Betrieb einer journalistischen Webseite definiert werden. Auch ist der Zugriff auf diese Informationen zu „kompatiblen Zwecken“ abzulehnen.
- Datenschutzfreundliche Voreinstellungen von Kommunikationssoftware würden die Rechte der Betroffenen wirksam und praktikabel schützen und damit die Datenschutz-Grundverordnung in sinnvoller und notwendiger Weise ergänzen. Die vorgeschlagene Streichung des Artikels 10 ePrivacy-Verordnung lehnt der vzbv daher ab.

HINTERGRUND

Mit der ePrivacy-Verordnung will die Europäische Kommission (EU-Kommission) den Datenschutz und die Vertraulichkeit in der elektronischen Kommunikation verbessern. Das Europäische Parlament (EU-Parlament) hat seine Position im Oktober 2017 abgestimmt, der Rat der Europäischen Union (EU-Rat) im Februar 2021. Bedauerlich ist jedoch, dass die Positionen des EU-Rats viele Ansätze enthalten, die aus Verbrauchersicht inakzeptabel sind.

Um den Schutz der Privatsphäre der Verbraucher auch künftig zu gewährleisten, sollten daher folgende Kernpositionen des vzbv in den anstehenden Trilog-Verhandlungen durch den europäischen Gesetzgeber dringend berücksichtigt werden.

[1] Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

VERARBEITUNG VON ELEKTRONISCHEN KOMMUNIKATIONSDATEN

Nach dem Vorschlag der EU-Kommission und des EU-Parlaments soll die Verarbeitung von elektronischen Kommunikationsdaten – also den Inhalten und Metadaten einer elektronischen Kommunikation – nur auf Grundlage eines gesetzlichen Erlaubnistatbestands oder mit Einwilligung der Nutzer möglich sein. Schon eine solche Regelung würde eine deutliche Ausweitung der bisherigen Verarbeitungsmöglichkeiten für Telekommunikationsunternehmen bedeuten. Denn bisher war die Verarbeitung von Inhalten nicht gestattet und die Verarbeitung von Metadaten nur in weitaus engeren Grenzen erlaubt.

Nach den Vorschlägen des EU-Rats soll jedoch die Weiterverarbeitung elektronischer Kommunikationsmetadaten ohne Einwilligung der Verbraucher deutlich erleichtert werden. So sollen Standortdaten zu wissenschaftlichen Zwecken sowie zu nicht weiter definierten „statistischen Zwecken“ verarbeitet werden, wenn diese Daten pseudonymisiert wurden und kein Profil der betroffenen Person erstellt wird. Jegliche andere Metadaten dürfen zu diesen Zwecken verarbeitet werden, wenn dies im Einklang mit europäischer Gesetzgebung oder nationalen Gesetzgebungen steht – eine eigene Rechtsgrundlage scheint nicht erforderlich zu sein, womit die Datenschutz-Grundverordnung unterlaufen wird. Auch sind im Text keine weiteren Schutzmaßnahmen enthalten, wie etwa Verpflichtungen zur Datenschutz-Folgenabschätzung, zur Konsultation der Aufsichtsbehörden, zur Information der Nutzer oder zur Bereitstellung von Widerspruchsmöglichkeiten.

Darüber hinaus soll die zweckändernde Weiterverarbeitung jeglicher pseudonymer Kommunikationsmetadaten grundsätzlich zulässig sein, wenn die Datenverarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben wurden. Die aufgeführten Schutzmaßnahem fallen äußerst schwach aus. So soll beispielweise eine Profilbildung möglich sein, solange die Profile keine rechtlichen oder anderen erheblichen Auswirkungen auf die Betroffenen haben. Demnach könnten beispielsweise Telekommunikationsanbieter künftig zu kommerziellen Zwecken verarbeiten, welche IP-Adressen (und damit Webseiten) von ihren Kunden aufgerufen werden. Auch hier sind darüber hinaus die zuvor genannten Schutzmaßnahmen nicht vorgesehen. Unklar ist außerdem, wie verhindert werden soll, dass beispielsweise Informationen von Journalisten, Ärzten, Rechtsanwälten oder Seelsorgern erfasst werden.

Vielmehr hat der Europäische Gerichtshof ausdrücklich in mehreren Urteilen ausdrücklich festgestellt, dass durch Kommunikationsmetadaten sehr sensible und persönliche Informationen offengelegt werden können, und dass diese Daten somit eine besondere Schutzwürdigkeit haben.[2] Dieser Schutzwürdigkeit werden die Regelungen nicht gerecht. Somit untergraben die Vorschläge des EU-Rats die Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten.

[2] Siehe verbundene Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger und andere, ECLI:EU:C:2014:238; verbundene Rechtssachen C-203/15 und C-698/15 Tele2 Sverige AB und Secretary of State for the Home Department, ECLI:EU:C:2016:970.

Ein Kompromiss zwischen den Positionen könnten Ansätze darstellen, die von der n bulgarischen Ratspräsidentschaft[3] sowie der Deutschen Bundesregierung[4] vorgeschlagen wurden. Demnach könnten einzig pseudonyme, auf Standortdaten begrenzte Metadaten zu wissenschaftlichen Zwecken oder für statistische Zählung unter Beachtung von Schutzvorgaben durch Telekommunikationsanbieter verarbeitet werden. Diese dürften die Daten aber nicht dazu verwenden, eine betroffene Person zu charakterisieren oder ein Profil über diese zu erstellen. Außerdem dürften die Daten keine sensitiven Informationen, wie Gesundheitszustände oder politische Ansichten offenbaren und müssten nach Erreichen des Zwecks anonymisiert oder gelöscht werden. Eine Übermittlung der Daten an Dritte wäre untersagt. Darüber hinaus müsste vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchgeführt und die zuständige Aufsichtsbehörde konsultiert werden. Den Betroffenen müsste außerdem ein Widerspruchsrecht zugestanden werden. Der vzbv erachtet diese Kompromissvorschläge zwar als sehr weitreichend, jedoch bewegen sich diese im Rahmen der Europäischen Grundrechtecharta und der Rechtsprechung des Europäischen Gerichtshofs.

> Ein Zurück hinter das Schutzniveau der bisherigen ePrivacy-Richtlinie ist nur in eng begrenzten Fällen unter strengen Voraussetzungen akzeptabel. Eine Weiterverarbeitung von elektronischen Kommunikationsmetadaten für „kompatible Zwecke“ ist in diesem besonders sensiblen Bereich aber nicht vertretbar und nicht mit der Rechtsprechung des Europäischen Gerichtshofs vereinbar. Daher lehnt der vzbv entsprechende Vorschläge vehement ab.

SCHUTZ DER MIT DEN GERÄTEN DER NUTZER IN VERBINDUNG STEHENDEN INFORMATIONEN („TRACKING“)

Auch hinsichtlich der Diskussion um den Schutz der mit den Geräten der Nutzer in Verbindung stehenden Informationen betont der vzbv, dass bereits die Vorschläge der EU-Kommission und des EU-Parlaments hinter den bisherigen Vorgaben der ePrivacy-Richtlinie zurückbleiben. Der vzbv trägt jedoch Ausnahmen mit, die sich auf die Reichweitenmessung beziehungsweise Webseitenanalyse durch den Anbieter oder im Rahmen einer Auftragsverarbeitung bei geeigneten Schutzmaßnahmen erstrecken. Eine Ausweitung auf weitere Rechtsgrundlagen, auch für pseudonyme Informationen, lehnt der vzbv ab.

Kritisch ist insbesondere, dass der Zugriff auf Nutzergeräte stets als erforderlich für die Erbringung eines Dienstes der Informationsgesellschaft erachtet werden soll, wenn es sich dabei um eine werbefinanzierte Nachrichtenseite handelt. Damit wird der Erforderlichkeitsbegriff entgegen bisheriger Auslegungen der Datenschutzaufsichtsbehörden unerträglich ausgedehnt und das Schutzniveau vor Tracking und Profiling im Internet weit unter die Regelungen der bisherigen ePrivacy-Richtlinie sowie der DSGVO abgesenkt.

[3] Vgl. Dokument 8537/18 der Bulgarischen Ratspräsidentschaft vom 12. Juni 2018.
[4] Vgl. Dokument 8864/2019 der Deutschen Bundesregierung vom 25. Juli 2019.

Darüber hinaus möchte der Rat auch hinsichtlich der Informationen, die auf den Endgeräten der Nutzer gespeichert sind, eine Verarbeitung zu „kompatiblen Zwecken“ ermöglichen. Auch wenn gewisse Schutzmaßnahmen vorgesehen sind – beispielsweise, dass aus den Daten kein Nutzerprofil erstellt werden darf – ist dieser Vorschlag abzulehnen. Denn es ist völlig unklar, welcher Zweck mit einer solchen unbestimmten Regelung verfolgt werden soll. Vielmehr sollten die spezifischen Zwecke ausdrücklich aufgeführt werden, um Rechtssicherheit und das höchstmögliche Maß an Schutz zu gewährleisten.

Im Kern geht es bei den Vorschlägen des EU-Rats also darum, die bisher in Deutschland gängige Praxis des Trackings zu Werbezwecken – ohne Einwilligung der Betroffenen und mit geringen Schutzmaßnahmen – beizubehalten beziehungsweise auszuweiten. Dabei wurde diese Praxis erst jüngst durch Urteile des Europäischen Gerichtshofs[5] sowie des Bundesgerichtshofs[6] für unzulässig erklärt. Denn nach geltendem Recht ist die Einwilligung durch die Betroffenen in ein solches Tracking erforderlich. Auch als Reaktion auf diese Urteile ist bereits eine Veränderung im Markt zu beobachten. Verbraucher erhalten immer häufiger die Entscheidungsmöglichkeit, ob ihre Interessen und ihr Verhalten zu Werbezwecken nachverfolgt werden dürfen. Wenngleich es auch hierbei weiterhin kritische Punkte gibt[7][8], ist es doch zu begrüßen, dass nicht mehr automatisch vorausgesetzt wird, dass die Nutzer mit diesen Praktiken einverstanden wären. Die Vorschläge des EU-Rats würden somit positive Entwicklungen konterkarieren, deutlich hinter der bisherigen Rechtslage zurückbleiben und damit die Praktiken der Online-Werbeindustrie vielmehr erleichtern, statt erschweren – zu Lasten aller Verbraucher.

Durch die Befürworter der Position des EU-Rats wird als Argument hervorgebracht, dass (journalistischen) Angeboten nicht ihre Finanzierungsquelle entzogen werden dürfte. Außerdem würden durch strenge Regelungen vor allem die Unternehmen Google und Facebook gestärkt werden, da es diesen leichter fallen würde, eine Einwilligung ihrer Nutzer in das Tracking zu erhalten.

Dabei ist die Frage durchaus umstritten, ob verhaltensbezogene Werbeformen als Finanzierungsquelle für journalistische Angebote tatsächlich alternativlos sind oder ob auch andere Werbe- und Finanzierungsmodelle denkbar sind. So legt beispielsweise eine akademische Studie aus den USA vom Mai 2019 nahe, dass das Tracking der Leserschaft lediglich zu einer 4-prozentigen Umsatzsteigerung bei journalistischen Angeboten führt.[9] Eine andere Studie wurde durch das Wirtschaftsprüfungsunternehmen PWC im Mai 2020 für den britischen Verband der Werbetreibenden ISBA durchgeführt. Darin kommen die Wirtschaftsprüfer zu dem Ergebnis,

---

[5] EuGH, Urteil vom 01.10.2019 - Rs. C-673/17; URL: https://curia.europa.eu/juris/liste.jsf?language=de&num=C-673/17 [Zugriff: 15.04.2021].

[6] BGH, Urteil vom 28.05.2020 – Rs. I ZR 7/16; URL: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html [Zugriff: 15.04.2021].

[7] Vgl. Matte, Célestin; Bielova, Nataliia; Santos, Cristiana: Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework (2019); URL: https://arxiv.org/pdf/1911.09964v1.pdf [Zugriff: 15.04.2021].

[8] Vgl. Eberl, Matthias: Pur-Abos im Test - Nicht ganz ohne (2020); URL: https://netzpolitik.org/2020/nicht-ganz-ohne/ [Zugriff: 15.04.2021].

[9] Vgl. Marotta, Veronica; Abhishek, Vibhanshu; Acquisti, Alessandro: Online Tracking and Publishers’ Revenues: An Empirical Analysis (2019); URL: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf [Zugriff: 15.04.2021].

dass nur etwa 50 Prozent der investierten Werbegelder auch tatsächlich die Verlage erreichte, auf deren Webeseiten die Werbung ausgespielt wurde. Der Verbleib von 15 Prozent der Gelder war darüber hinaus nicht mehr nachvollziehbar.[10] Dementsprechend konnten auch verschiedene Medienunternehmen – wie zum Beispiel die New York Times[11] oder der niederländische öffentlich-rechtliche Rundfunk[12] – laut Presseberichten jüngst Umsatzsteigerungen verbuchen, nachdem sie sich von verhaltensbezogenen Werbeformen zurückgezogen haben und sich auf andere Werbemodelle konzentrieren.

Der bedenklichen Marktmacht von Facebook und Google kann hingegen nicht damit begegnet werden, das grundrechtliche verankerte Schutzniveau der Menschen in Europa abzusenken. So hat der Bundesgerichtshof erst jüngst in einer vorläufigen Entscheidung festgestellt, dass Facebook seine marktbeherrschende Stellung missbraucht, indem es Nutzungsbedingungen verwendet, die nicht den Vorgaben der Datenschutz-Grundverordnung entsprechen. Denn Facebook lasse seinen Nutzern keine Wahl, ob sie die Plattform auch nutzen können, ohne dass Facebook ihre Verhaltensweisen und Interessen auch auf anderen (unter anderem journalistischen) Webseiten im Internet erfasst.[13]

Auch die aktuellen Pläne von Google, künftig keine Drittanbieter-Cookies mehr zu unterstützen, sondern das Tracking der Nutzer seines Chrome-Browsers in den Browser zu verlagern, zeigt die Notwendigkeit von strikten Regelungen in der ePrivacy-Verordnung auf. Denn würden die datenschutzrechtlichen Anforderungen für das Tracking im Internet abgesenkt werden, würde es dem Unternehmen noch einfacher als bisher fallen, seine Marktmacht weiter auszubauen und auszunutzen.

Zudem besteht das Risiko, dass Unternehmen wie Facebook und Google ihre Markt- und Datenmacht in neue „benachbarte“ Märkte ausdehnen, indem sie Daten aus verschiedenen Lebensbereichen/Sektoren kombinieren und sich so einen Wettbewerbsvorteil in neuen Märkten verschaffen, dem kleinere Wettbewerber kaum standhalten können. Entscheidend ist es daher vielmehr, für eine wirksame Durchsetzung der wettbewerbs- und datenschutzrechtlichen Vorgaben zu sorgen beziehungsweise wirksamere Wettbewerbsregeln zu schaffen.

> Die ePrivacy-Verordnung darf nicht hinter der bisherigen Rechtslage zurückbleiben. Das Speichern von Informationen auf beziehungsweise der Abruf solcher Informationen von den Geräten der Nutzer darf nicht als erforderlich für den Betrieb einer journalistischen Webseite definiert werden. Der Zugriff auf diese Informationen zu „kompatiblen Zwecken“ ist abzulehnen. Der Schutz der Verbraucher kann nur gewährleistet werden, wenn der Zugriff auf diese Informationen

[10] Vgl. ISBA: Programmatic supply chain transparency study (2020), S. 8, URL: https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf [Zugriff: 15.04.2021].
[11] Vgl. Davies, Jessica: After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue (2019); URL: https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/ [Zugriff: 15.04.2021].
[12] Vgl. Lomas, Natasha: Data from Dutch public broadcaster shows the value of ditching creepy ads (2020); URL: https://techcrunch.com/2020/07/24/data-from-dutch-public-broadcaster-shows-the-value-of-ditching-creepy-ads/ [Zugriff: 15.04.2021].
[13] BGH, Beschluss vom 23.06.2020 – Rs. KVR 69/19; URL: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html?nn=10690868 [Zugriff: 15.04.2021].

ausschließlich zu gesetzlich festgelegten Zwecken unter strikten Bedingungen oder auf Basis der Einwilligung erfolgen darf.

DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Der EU-Rat spricht sich für die Einführung einer Regelung zu Browsereinstellungen 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.

Jedoch greift der Vorschlag des EU-Rats deutlich zu kurz. Eine solche Regelung würde Anbieter von datenschutzfreundlichen Browsern benachteiligen, da sie eines der Alleinstellungsmerkmale solcher Anbieter verwässern würde. Nutzer, die durch die derzeitige manipulative Gestaltung der Einwilligungsbanner genervt auf „akzeptieren“ klicken, könnten sich nicht mehr drauf verlassen, durch die Einstellungen ihrer Webbrowser vor individualisiertem Tracking zu Werbezwecken geschützt zu sein. Gleichzeitig würde eine solche Regelung den derzeitigen Marktführer Google Chrome bevorzugen, der von Seiten des Herstellers nicht datenschutzfreundlich voreingestellt ist. Darüber hinaus ist völlig unklar, wie ein Webbrowser erkennen sollte, dass eine Einwilligung, die ein Verbraucher gegenüber einem Webseitenbetreiber erteilt hat, tatsächlich den strikten Anforderungen der DSGVO entspricht.

Um den Schutz personenbezogener Daten sowie den Schutz der Privatsphäre der Verbraucher zu gewährleisten, bedarf es vielmehr 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-Verordnung keine Einwilligung erforderlich ist, sollten per Voreinstellung gespeichert und abgerufen werden dürfen. Außerdem sollten Unternehmen verpflichtet werden, ein Tracking der Verbraucher – sowie entsprechende Anfragen – zu unterlassen, wenn die Nutzer aktiv den „Do-not-Track“-Mechanismus ihres Webbrowsers aktivieren.

Der vzbv ist auch der Ansicht, dass die Softwarehersteller dazu verpflichtet werden sollten, die Entscheidungen der Verbraucher technisch abzubilden. So sollte ein Whitelisting von Webseiten, beispielsweise bei Erteilung einer Einwilligung zur Reichweitenmessung, einfach möglich sein. Jedoch muss ein solches Whitelisting – wie auch die Einwilligung als solche – granular erfolgen. 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 des Verordnungsvorschlags eine Einwilligung

erforderlich ist und Informationen, bei denen dies nicht der Fall ist. In der Praxis erfolgt darüber hinaus beispielsweise das Tracking zu Werbezwecken zum Teil auch über Erstanbieter-Cookies.[14]

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.[15] 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.[16] Datenschutzfreundliche Voreinstellungen schützen also in erster Linie diese besonders vulnerablen Verbrauchergruppen. Daher ist es nicht akzeptabel, dass Artikel 10 des Verordnungsvorschlags durch den EU-Rat gestrichen wurde, der eine Verpflichtung für Hersteller von Kommunikationssoftware vorsah, ihre Produkte datenschutzfreundlich zu gestalten.

> Datenschutzfreundliche Voreinstellungen von Kommunikationssoftware würden die Rechte der Betroffenen wirksam und praktikabel schützen und damit die Datenschutz-Grundverordnung in sinnvoller und notwendiger Weise ergänzen. Die vorgeschlagene Streichung des Artikels 10 des Verordnungsvorschlags lehnt der vzbv daher ab.

Kontakt

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien
digitales@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

[14] 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: 15.04.2021].
[15] Europäische Kommission: Flash Eurobarometer 443 (2016); S. 46; URL: https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG [Zugriff: 15.04.2021].
[16] Ebenda; S. 37.