verbraucherzentrale
Bundesverband

ANWENDBARKEIT DES TELEMEDIENGESETZES

Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zur Positionsbestimmung der Datenschutzkonferenz „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“

28. Juni 2018

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Team Digitales und Medien

Markgrafenstraße 66
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. HINTERGUND

Seit dem 25. Mai 2018 wird die Datenschutz-Grundverordnung (DSGVO) angewendet, jedoch verzögern sich die Verhandlungen zur ePrivacy-Verordnung, die die bisherige ePrivacy-Richtlinie ersetzen wird. Daher besteht dringender Klärungsbedarf hinsichtlich der Frage, in welchem Verhältnis das Telemediengesetz (TMG) – und hier insbesondere die Regelungen des § 15 Absatz 3 TMG – zur DSGVO und zur ePrivacy-Richtlinie stehen und welche Bestimmungen in der Übergangszeit anzuwenden sind.

Der Verbraucherzentrale Bundesverband (vzbv) begrüßt daher die Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) zur Anwendbarkeit des TMG. Allerdings sieht der vzbv an einigen Stellen weiteren Klärungsbedarf und bedankt sich daher für die Gelegenheit, zu diesen wichtigen Fragen Stellung beziehen zu können.

II. DIE POSITIONEN IM EINZELNEN

1. VORRANG DER DSGVO GEGENÜBER DEM TMG

Der vzbv stimmt der DSK zu, dass die DSGVO grundsätzlich Vorrang vor dem bestehenden nationalen Recht hat und dementsprechend §§ 12, 13, 15 TMG nicht mehr anwendbar sind. Abschnitt 4 des TMG stellt keine Umsetzung der ePrivacy-Richtlinie dar. Daher besteht kein Anwendungsvorrang des TMG auf Basis des Artikels 95 DSGVO. Diese Auffassung wird nicht nur von der DSK und von Verbraucherschutzorganisationen vertreten, sondern unter anderem auch von hochrangigen Vertretern der EU-Kommission geteilt.[1] §§ 12, 13, 15 TMG setzen also in erster Linie die bisherige Datenschutz-Richtlinie um und werden somit durch die DSGVO verdrängt.

Selbst wenn man von einer vollständigen Umsetzung der ePrivacy-Richtlinie im TMG ausgehen würde, wäre fraglich, ob das TMG im betroffenen Bereich einen Anwendungsvorrang genießen würde. Denn Artikel 95 DSGVO bezieht sich lediglich auf die „Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen“. Der Begriff der „elektronischen Kommunikationsdienste“ wird in Artikel 2 lit. a) der Rahmenrichtlinie[2] definiert und schließt explizit Dienste aus, „die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben”.

2. KEINE DIREKTE ANWENDBARKEIT DER EPRIVACY-RICHTLINIE

Ferner stimmt der vzbv der DSK zu, dass die ePrivacy-Richtlinie nicht direkt anwendbar ist und dementsprechend als Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten zu Zwecken des Trackings, Profilings und Targetings, Artikel 6 Absatz 1 lit. a), b) und f) DSGVO heranzuziehen sind.

---

[1] Vgl. *Selmayr* zitiert in: *Dix, Kipker* (2018): „EAID: Die ePrivacy-Verordnung auf der Zielgeraden?“; in: ZD-Aktuell 2018, 04281

[2] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)

3. MÖGLICHE RECHTSGRUNDLAGEN DER DSGVO FÜR DIE ÜBERTRAGUNG VON NACHRICHTEN ODER ZURVERFÜGUNGSTELLUNG VON TELEMEDIEN

Unstrittig dürfte sein, dass es auf Basis von Artikel 6 Absatz 1 lit. b) oder f) DSGVO zulässig ist, personenbezogene Daten zu verarbeiten, wenn dies technisch erforderlich ist, um eine Nachricht über ein elektronisches Kommunikationsnetz zu übertragen oder um einen Telemediendienst zur Verfügung zu stellen. Dies ist beispielsweise grundsätzlich bei Warenkörben im elektronischen Handel oder bei Anpassungen der Benutzeroberfläche der Fall.

4. RECHTSGRUNDLAGE DER INTERESSENABWÄGUNG FÜR TRACKING, PROFILING UND TARGETING

Hinsichtlich der Frage, inwieweit Tracking, Profiling und Targeting auf der Rechtsgrundlage der Interessenabwägung nach Artikel 6 Absatz 1 lit. f) durchgeführt werden können, besteht jedoch weiterer Klärungsbedarf.

Erwägungsgrund (EWG) 47 DSGVO betont, dass bei der Beurteilung, ob die berechtigten Interessen eines Verantwortlichen oder eines Dritten an einer Verarbeitung den Interessen oder den Grundrechten und Grundfreiheiten der betroffenen Personen überwiegen, *die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen* sind. Ein berechtigtes Interesse kann laut EWG 47 beispielsweise dann vorliegen, *wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, zum Beispiel wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht*.

Für Verbraucherinnen und Verbraucher[3] sind viele der derzeitigen Datenverarbeitungen zu Werbezwecken online jedoch nicht zu erwarten. Zwar dürfte ein durchschnittlich informierter Verbraucher darüber informiert sein, dass seine personenbezogenen Daten im Internet verarbeitet werden, um scheinbar kostenfreie Angebote über Werbung zu finanzieren (auch wenn sich nur 29 Prozent der Deutschen damit wohlfühlen[4]). Allerdings muss bei einem Großteil der Bevölkerung bezweifelt werden, dass sie sich angesichts der Komplexität der Systeme und der Undurchsichtigkeit des Datenaustausches über die verwendeten Techniken und den Umfang der Datenverarbeitung bewusst sind. So wissen beispielsweise laut des D21 Digital Index 2017/2018 nur 58 Prozent der über 14-Jährigen in etwa, was ein Cookie ist.[5] In einer repräsentativen Befragung, die Yougov im Auftrag der Plattform Verimi im Frühjahr 2018 durchführte, stimmten 67 Prozent der Teilnehmer der Aussage zu, gar nicht zu wissen, was im Internet mit ihren persönlichen Daten passiert.[6]

Darüber hinaus bestehen zwischen den Betroffenen und den für die Datenverarbeitung Verantwortlichen im Bereich der Internetwerbung oftmals keine maßgeblichen und angemessenen Beziehungen im Sinne des EWG 47 DSGVO, die eine Datenverarbeitung

---

[3] Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[4] Europäische Kommission (2015): Special Eurobarometer 431, Seite 40

[5] D21-Digital-Index 2017 / 2018, eine Studie der Initiative D21, durchgeführt von Kantar TNS, Seite 21

[6] Verimi GmbH (2018): Datensicherheit im Internet: Nutzer fühlen sich kaum geschützt, wünschen sich anderseits bequeme Anwendungen. https://www.presseportal.de/pm/128971/3976690, 21.06.2018

auf Basis der Interessenabwägung rechtfertigen würden. Im Gegenteil übermitteln nahezu alle Top-Webseiten Daten an Drittanbieter oder laden Code von Dritten auf die Geräte der Nutzer.[7] Auf mobilen Endgeräten sieht die Lage nicht anders aus. Nahezu alle Top-Apps haben ein oder mehrere Tracking-Frameworks Dritter eingebunden.[8]

Aus Sicht des vzbv wird eine Datenverarbeitung zu Zwecken der Direktwerbung nicht per se durch die DSGVO privilegiert. EWG 47 DSGVO besagt lediglich, dass eine solche Verarbeitung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden *kann*. Anders als etwa die Betrugserkennung (ebenso EWG 47) wird Direktwerbung eben nicht automatisch als berechtigtes Interesse anerkannt.

Ferner ist fraglich, ob es sich bei Internetwerbeformen, wie beispielsweise dem Targeting, überhaupt um Direktwerbung handelt. Laut des Bundesgerichtshofs ist Direktwerbung gegeben, „wenn der Werbende einen *unmittelbaren Kontakt zu einem bestimmten Adressaten* herstellt, sei es durch *persönliche Ansprache*, Briefsendungen oder durch Einsatz von Telekommunikationsmitteln wie Telefon, Telefax oder E-Mail."[9]

Auch die EU-Kommission definiert in ihrem Vorschlag zur ePrivacy-Verordnung Direktwerbung über elektronische Kommunikationsdienste lediglich als „jede Art der Werbung in schriftlicher oder mündlicher Form, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet wird, auch mittels automatischer Anruf- und Kommunikationssysteme mit oder ohne menschliche(r) Beteiligung, mittels E-Mail, SMS-Nachrichten usw."[10][11] Würden Internetwerbeformen, wie beispielsweise das Targeting, unter dem Begriff der Direktwerbung erfasst sein, müssten auch die strengen Vorgaben des künftigen Artikels 16 ePVO auf diese Werbeformate angewendet werden. Dies scheint jedoch politisch nicht gewünscht zu sein.

Auch kann nicht pauschal angenommen werden, dass Tracking, Profiling und Targeting weniger in die Grundrechte und Grundfreiheiten der Betroffenen eingreifen, als beispielsweise Direktwerbung per Briefsendungen oder mittels elektronischer Kommunikationsdienste. Selbst wenn Tracking, Profiling und Targeting pseudonymisiert vorgenommen werden, kann der Einsatz dieser Technologien für die Betroffenen deutlich manipulativer, intransparenter und schwerer zu kontrollieren sein, als die klassische Direktwerbung. So kann Internetwerbung gezielt auf die Wünsche, Interessen und Bedürfnisse von Betroffenen zugeschnitten werden. Für die meisten Verbraucher dürfte es aber oftmals unmöglich sein, abzuschätzen, inwieweit Internetwerbung auf sie zugeschnitten ist und welche Informationen aus welchen Quellen eingeflossen sind.

Eine Pseudonymisierung schützt die Betroffenen in diesem Zusammenhang nur sehr begrenzt. Sie mindert zwar das Risiko der Verarbeitung, dennoch kann es weiterhin

---

[7] Vgl. *Libert* (2015): Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites; in: International Journal of Communication 9(2015), Seite 3551

[8] Vgl. *Seneviratne, Suranga* (2015): Short: A Measurement Study of Tracking in Paid Mobile Applications; in: WiSec '15 Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Article No. 7

[9] BGH, Urteil v. 15.12.2015, Az. VI ZR 134/15

[10] Artikel 4 Absatz 3 lit. f) ePVO

[11] Das EU-Parlament definiert: „jede Art der Werbung in schriftlicher oder mündlicher Form oder als Videoformat, die an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet, für sie bereitgestellt oder ihnen angezeigt wird, auch mittels automatischer Anruf- und Kommunikationssysteme mit oder ohne Beteiligung eines Menschen, mittels E-Mail, SMS-Nachrichten, Faxgeräten usw.;"
Eine Definition des EU-Rates steht noch aus

möglich sein, Betroffene auszusondern, pseudonyme Profile mit weiteren Daten anzureichern oder diese mit weiteren Informationen zu verketten, beispielsweise über das Cross-Domain-Tracking, Cross-Device-Tracking oder Cookie Syncing.[12]

Zu bedenken – und zu adressieren – ist hierbei die Vielfalt und Eingriffstiefe der verwendeten Technologien. Studien belegen unter anderem die gängige Verwendung von Storage-basierten oder Cache-basierten Trackingmechanismen[13], Device- und Browser-/Canvas-Fingerprinting[14], User-IDs[15], Werbemodulen (SDKs)[16], Addressable TV[17], Ultrasonic Tracking[18], Unique Identifier Headern („Zombie-Cookies“)[19], … sowohl auf PCs, als auch mobilen Endgeräten, Smart Home Devices oder IoT-Geräten. Auch zeigen diese Studien, dass gegen viele dieser Technologien – und noch viel weniger gegen die Summe dieser Technologien – für durchschnittlich informierte Verbraucher kaum Transparenz und kaum Schutzmöglichkeiten bestehen. In jedem Fall dürften diese Schutzmöglichkeiten deutlich schwächer ausfallen, als gegen eine Datenverarbeitung zu Zwecken der klassischen Direktwerbung.

> Basierend auf diesen Erwägungen kann Tracking, Profiling und Targeting nur in begrenzten Fällen auf die Rechtsgrundlage der Interessenabwägung gestellt werden.

Dies kann beispielsweise der Fall sein, wenn die Datenverarbeitung erforderlich ist,

- um einen vom Nutzer angeforderten Dienst nach den Bedürfnissen der Nutzer zu gestalten (wie zum Beispiel eine vom Nutzer gewünschte Personalisierung der Angebote),
- für die statistische Zählung des eigenen Webpublikums beziehungsweise der Reichweitenmessung, um den Nutzungsumfang der eigene Angebote abschätzen zu können,
- um Werbung für eigene Produkte zu schalten und um die Wirksamkeit der Werbung zu analysieren

---

[12] Vgl. *Englehardt*, *Narayanan* (2016): Online Tracking: A 1-million-site Measurement and Analysis; in: CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Seite 1388-1401

[13] Vgl. *Bujlow* et al. (2017): Web Tracking: Mechanisms, Implications and Defenses; in: Proceedings of the IEEE (Volume: 105, Issue: 8, Aug. 2017), Seite 1476 - 1510

[14] Vgl. *Bujlow* et al. (2017): Web Tracking: Mechanisms, Implications and Defenses; in: Proceedings of the IEEE (Volume: 105, Issue: 8, Aug. 2017), Seite 1476 - 1510
Vgl. *Englehardt*, *Narayanan* (2016): Online Tracking: A 1-million-site Measurement and Analysis; 2016; in: CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Seite 1388-1401

[15] Vgl. *Razaghpanah* et al. (2018): Apps, Trackers, Privacy, and Regulators. A Global Study of the Mobile Tracking Ecosystem; in: Proceedings of Network and Distributed Systems Security (NDSS) Symposium 2018

[16] Vgl. *Rehberg* (2017): Was hat es mit den Modulen in Android Apps auf sich?; https://android.izzysoft.de/articles/named/app-modules-1?lang=de, 20.06.2018

[17] Medienkorrespondenz (2017): Wenn per Fernseher Nutzerdaten gesammelt werden: DLM sieht Addressable TV in Konflikt mit Datenschutz; https://www.medienkorrespondenz.de/politik/artikel/wenn-per-fernseher-nutzerdaten-gesammelt-werden-dlmnbspsieht-addressablenbsptv-in-konflikt-mit.html, 20.06.2018

[18] Vgl. *Arp, et al.* (2017): Privacy Threats through Ultrasonic Side Channels on Mobile Devices; in: 2017 IEEE European Symposium on Security and Privacy (EuroS&P)

[19] Vgl. Access Now (2015): The Rise of Mobile. Tracking Headers: How Telcos Around the World Are. Threatening Your. Privacy

und dabei (neben den allgemeinen Vorgaben der DSGVO)

- die Datenverarbeitung durch den Verantwortlichen selbst oder im Rahmen einer Auftragsverarbeitung durchgeführt wird und
- personenbezogene Daten Dritten nicht offengelegt werden und
- Profile nicht mit Informationen aus Drittquellen angereichert oder über verschiedene Kontexte hinweg verkettet werden und
- die Betroffenen über wirksame Möglichkeiten verfügen, der Datenverarbeitung umfassend, vollständig, einfach und auf Dauer zu widersprechen[20] und vom Verantwortlichen Widersprüche mittels automatisierter Verfahren (wie dem Do-Not-Track-Standard) akzeptiert werden und
- die Verarbeitung für die Betroffenen transparent[21] ist und sie auf ihr Widerspruchsrecht hingewiesen wurden und
- lediglich pseudonyme Daten verarbeitet werden und
- keine Rückschlüsse auf besondere Kategorien personenbezogener Daten gezogen werden können und
- die Daten unverzüglich nach Zweckerfüllung anonymisiert oder gelöscht werden.

5. RECHTSGRUNDLAGE DER EINWILLIGUNG FÜR TRACKING, PROFILING UND TARGETING

Soll Tracking, Profiling und Targeting auf der Rechtsgrundlage der Einwilligung durchgeführt werden, sind die Anforderungen der Artikel 4 Nummer 11, Artikel 6 Absatz 1 lit. a), Artikel 7 und Artikel 8 DSGVO zu beachten (freiwillig, spezifisch, informiert, unmissverständlich, vor der Verarbeitung). [22] Dies schließt eine konkludente Einwilligung oder eine Kopplung der Einwilligung aus. Die Verantwortlichen müssen ferner den Nachweis erbringen, dass technische und organisatorische Maßnahmen getroffen wurden, um entsprechende Einwilligungen nach den Vorgaben der DSGVO einzuholen.

6. ACHTUNG DER GRUNDSÄTZE DER DSGVO

Ungeachtet der gewählten Rechtsgrundlage müssen sich alle Datenverarbeitungen an den Grundsätzen des Artikels 5 DSGVO orientieren, wie insbesondere der Verarbeitung nach Treu und Glauben, der Transparenz, der Zweckbindung, der Datenminimierung und der Speicherbegrenzung. Techniken, mit denen beispielsweise das Verhalten der Betroffenen umfassend erfasst und analysiert wird (wie zum Beispiel beim Tracking des Klickstreams), mit denen die Präferenzen der Betroffenen aktiv umgangen werden (wie zum Beispiel bei der Verwendung von Unique Identifier Headern oder anderen „Evercookies“ oder „Zombie Cookies“) oder mit denen die physische Umgebung der Betroffenen und Dritter analysiert wird (wie zum Beispiel beim Ultrasonic Tracking), entsprechen diesen Grundsätzen nicht und sind daher mit der DSGVO nicht vereinbar.

---

[20] Nicht ausreichend als Transparenz- und Opt-Out-Mechanismus ist beispielsweise das AdChoices-System der europäischen Werbewirtschaft. Laut einer Studie der European Interactive Digital Advertising Alliance und TRUSTe aus dem Jahr 2015, haben lediglich etwa 10% der deutschen Internetnutzer zwischen 16-70 Jahren das „AdChoices-Symbol incl. Admarker-Text“ wahrgenommen. Von diesen haben nur etwa 25% auf das Icon geklickt – also etwa gerade einmal 2,5% der deutschen Internetnutzer https://www.trustarc.com/press/growing-awareness-oba-icon/, 20.06.2018

[21] Vgl. Artikel-29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679, WP260 rev.01

[22] Vgl. Artikel-29-Datenschutzgruppe, Guidelines on consent under Regulation 2016/679, WP259 rev.01