POSITIONSPAPIER

VAUNET
Verband Privater Medien

Stellungnahme zu den European Data Protection Board's (EDPB) Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Datum 17. Januar 2024

1. Vorbemerkungen

Der VAUNET – Verband Privater Medien e. V. bedankt sich für die Gelegenheit zur Stellungnahme zu den Guidelines 2/2023 des European Data Protection Board's (EDPB) bezüglich des technischen Anwendungsbereichs von Art. 5 (3) der ePrivacy Directive (ePD).

Der VAUNET ist der deutsche Spitzenverband privater Medienanbieter. Er vertritt über 160 Unternehmen, die privatwirtschaftlich journalistisch-redaktionell gestaltete Radio-, Fernseh- und Onlinemedien veranstalten. Mit ihren Angeboten bereichern seine Mitglieder Deutschlands und Europas Medienlandschaft durch Vielfalt, Kreativität und Innovation.

Der VAUNET unterstützt den Ansatz des EDPB, mittels der Guidelines zu einer klaren und damit rechtssicheren Auslegung des Anwendungsbereichs von Art. 5 (3) ePD beizutragen. Zugleich teilt der VAUNET uneingeschränkt das Anliegen, die Privatsphäre von Nutzern und die Vertraulichkeit privater Kommunikation zu schützen.

Private Medien sind als Anbieter von Online- und Mobile-Angeboten jedoch in besonderem Maße auf die erfolgreiche Nutzung ihrer Angebote bei gleichzeitiger effizienter Refinanzierbarkeit angewiesen. Essenziell hierfür ist der Einsatz innovativer datenbasierter Werbetechnologie. Bei der Auslegung von Art. 5 (3) ePD muss daher die unternehmerische Freiheit in hinreichendem Maße Berücksichtigung finden. Dies gilt vor allem im Rahmen der Verbreitung privater Medieninhalte. Durch Auslegung des Art. 5 (3) ePD entstehende Hürden für den Einsatz von Werbetechnologien und für die Kommunikation von Inhalten haben stets unmittelbar nachteilige Auswirkungen auf die Meinungs- und Medienvielfalt.

Der VAUNET nimmt vor diesem Hintergrund die Auslegung der für Art. 5 (3) ePD maßgeblichen Begriffe *„gaining access to"* und *„stored information"* durch den EDPB mit Besorgnis zur Kenntnis.

Sie birgt auf Grund ihrer Weite die Gefahr, jedwede Interaktion im Onlineumfeld entgegen Wortlaut, Schutzzweck und Systematik grundsätzlich unter Einwilligungsvorbehalt zu stellen. Dies führt zu innovationshemmenden und in der Praxis kaum zu überwindenden Hürden für die datenschutzkonforme Verbreitung von audio-visuellen Medieninhalten.

Der VAUNET regt daher an, die **weite Auslegung** der Begriffe *„gaining access to"* und *„stored information"* **aufzugeben**. Hierzu sollten vor allem die Ausführungen in Ziffern 2.5 und 2.6 der Leitlinien gestrichen bzw. angepasst werden.

Dies vorausgeschickt nimmt der VAUNET wie folgt Stellung:

2. EDPB-Auslegung führt in der Praxis zu widersprüchlichen Ergebnissen

Gemäß der Leitlinien soll der Anwendungsbereich von Art. 5 (3) ePD nicht nur den Zugriff auf Informationen, die im Endgerät gespeichert werden (wie z. B. Cookies) erfassen (Rn. 31 und 32 Leitlinien).

Vielmehr soll es für ein *„access to information"* ausreichen, wenn Informationen von einem Endgerät zu einem Empfänger außerhalb des Endgerätes gesendet werden (Rn. 33 der Leitlinien). Allein die Tatsache, dass eine technische Anweisung zur Zusendung von Informationen aus dem Endgerät besteht, eröffne den Anwendungsbereich von Art. 5 (3) ePD.

Zugleich sei unerheblich, wer die Informationen gespeichert oder die Zusendung der Informationen initialisiert habe. Dies gelte auch für die Dauer der Speicherung von Informationen im Endgerät. Folglich seien auch flüchtige Speichervorgänge (bspw. in RAM- und CPU) erfasst (Rn. 37 Leitlinien).

Der VAUNET lehnt diese Auslegung als zu weitgehend ab. Sie birgt die Gefahr, dass in der Praxis jegliche elektronische Kommunikation unter den Anwendungsbereich von Art. 5 (3) ePD fällt und damit grundsätzlich unter Einwilligungs- bzw. Rechtfertigungsvorbehalt gestellt wird. Denn in der Diktion des EDPB wären generische, protokollbasierte Kommunikationsanweisungen, durch welche Nutzerendgeräte Informationen versenden, um Kommunikation überhaupt erst zu ermöglichen, von Art. 5 (3) ePD erfasst.

Dies führt in der Praxis zu erheblichen Widersprüchen.

Beispielsweise müsste hinsichtlich der Internetkommunikation davon ausgegangen werden, dass jeder Aufruf einer Webseite oder eines Video- oder Audiobeitrags *„gaining access"* im Sinne des Art. 5 (3) ePD ist, da hierbei IP-Adressen durch den http-Header Request vom Endgerät versendet werden.

Gleiches wäre u. U. auch für die rundfunkspezifische Verbreitung audio-visueller Medieninhalte via HbbTV-Standard anzunehmen, da hier auf Basis von Application Information Table (AIT) ein Austausch von Informationen zwischen Endgerät (z. B. Smart-TV oder Set-Top-Box) und Anbieter erfolgt.

In beiden Fällen liegt jedoch bei technik- und realitätsnaher Auslegung kein *„Zugriff auf Informationen im Endgerät"* im Wortsinn und damit kein Zugriff in die Privatsphäre des Nutzers vor: Bei der Online-Kommunikation werden für den Kommunikationsablauf zwingend notwendige Informationen auf Grund des HTTP-Protokolls automatisiert übersendet. Bei Nutzung des HbbTV-Signals ist es der Nutzer, welcher durch den sog. „Red Button" auf der Fernbedingung die Zusendung von Informationen seines Endgeräts initialisiert.

3. Datenschutzrechtliche Anforderungen nicht realisierbar und innovationshemmend

Darüber hinaus führt die Auslegung des EDPB in der Praxis zu kaum überwindbaren Hürden für eine datenschutzkonforme Verbreitung von Medieninhalten.

Erstens müssten Medienanbieter, die auf Webseiten Video- und/oder Audioinhalte anbieten, mit der Auslegung des EDPB ***zu jedem einzelnen*** Verbindungsvorgang das Vorliegen einer DSGVO-konformen Einwilligung nachweisen (es sei denn, sie können darlegen, dass die Nutzung der Informationen unbedingt notwendig gewesen ist, um einen Dienst anzubieten, der ausdrücklich nachgefragt wurde).

Als Folge ist die Entstehung einer Vielzahl neuer Consent-Banner zu erwarten, die neben die bereits bestehenden Consent-Banner treten. Ein Ergebnis, dass auch unter Berücksichtigung der erheblichen Nachteile von Browservoreinstellungen sowohl aus Anbieter- als auch Verbraucherperspektive offensichtlich nicht wünschenswert ist. Hiermit stellen sich die Leitlinien in erheblichem Kontrast zur laufenden Diskussion rund um die Verhinderung der sog. „Cookie Fatigue".

Zweitens müssten Medienanbieter erforderliche Einwilligungen ***vor*** Zugriff bzw. Zusendung der fraglichen Informationen einholen. Für den Bereich der Internetkommunikation ist dies jedoch nicht möglich, da die Einwilligung vor dem Aufbau des die Kommunikation erst ermöglichenden Datenaustausches (HTTP Header Request) abgefragt werden müsste. Es bleibt nach den Leitlinien unklar, wie Anbieter diesen Anforderungen mithin überhaupt gerecht werden könnten.

Drittens müssten Webseitenbetreiber Einwilligungen für Verarbeitungsvorgänge einholen, die ***nicht von ihnen*** initialisiert worden sind, sondern auf Grund allgemeiner genereller Kommunikationsstandards (und daher auf Grund Dritter) vorgenommen werden. Dies führt auch mit Blick auf die Verantwortlichkeitsverteilung der DSGVO zu nicht auflösbaren datenschutzrechtlichen Friktionen.

Der VAUNET regt daher an, vorstehende Gesichtspunkte stärker als bisher in die Erstellung der Leitlinien einzubeziehen und dabei auch zu beachten, dass zu hoch angelegte datenschutzrechtliche Hürden innovationshemmend wirken. Dies gilt insbesondere auch in Bezug auf die Weiterentwicklung Privatsphäre freundlicher Werbetechnologien, wenn die gesetzliche Auslegung schon auf Grund ihrer Weite per se zu einem Einwilligungserfordernis führt.

4. Wortlaut, Sinn und Zweck sowie Systematik sprechen gegen weite Auslegung

Die vorgenommene weite Auslegung des *„gaining of access to information"* begegnet zudem rechtlichen Bedenken.

Zum einen ist die Auslegung nicht mit dem Wortlaut von Art. 5 Abs. 3 Satz 1 ePD vereinbar. Dieser spricht ausdrücklich von *„access to information"*. Nach allgemeinem Sprachgebrauch setzt *„access to"* eine aktive Handlung der zugreifenden Person voraus. Hätte der Europäische Gesetzgeber auch den passiven Empfang von Informationen in den Anwendungsbereich einbeziehen wollen, hätte er ein *„receipt of"* bzw. ein *„delivery of information"* aufnehmen können und müssen. Dies ist jedoch nicht geschehen.

Zum anderen spricht der aus Erwägungsgrund 24 ersichtliche Sinn und Zweck des Art. 5 Abs. 3 ePD gegen die vorgenommene Auslegung. Erwägungsgrund 24 ePD lautet:

> *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.* ***So called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge*** *in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned."* **(Hervorhebungen durch den Verfasser)**

Art. 5 Abs. 3 ePD soll im Kern also vor dem *„Eindringen"* („to enter") schädlicher Technologie auf einem Endgerät und damit in die Privatsphäre des Nutzers schützen. Schutzgegenstand ist folglich die Integrität des Endgerätes, die jedoch bei proaktiver und freiwilliger Zusendung von Informationen vom Endgerät nicht tangiert ist.

Auch systematische Gründe stehen der Auslegung entgegen. Mit der weiten Auslegung wäre bzgl. des Austausch von Informationen zur Etablierung von Kommunikation faktisch auch *„traffic data"* erfasst. *„Traffic data"* werden jedoch ausdrücklich in Art. 5 **Abs. 1 und 2** ePD adressiert und abschließend geregelt. Hieraus folgt, dass „traffic data" nicht auch von Art. 5 Abs. 3 ePD erfasst werden sollen.

Genauso wie die weite Auslegung des Begriffs *„gaining access to"* mithin keine rechtliche Grundlage hat, fehlt eine solche auch für die Ausweitung des Begriffes *„stored information"* auf bloß flüchtige Speichervorgänge. Der Begriff ***„stored*** *information"* enthält ersichtlich ein zeitliches Moment. Speicherungen müssen ***bereits*** auf dem Endgerät vorhanden sein, damit auf sie zugegriffen werden kann. Denklogisch sind daher Speicherungen nicht erfasst, die erst auf Grund eines Verarbeitungsvorgangs und nur für deren Zeitraum entstehen.

Vorstehende Erwägungen werde im Ergebnis auch seitens der deutschen Datenschutzbehörden bestätigt. Diese haben über die Datenschutzkonferenz (DSK) am 20. Dezember 2021 Orientierungshilfen für Telemedienanbieter veröffentlicht[1]. Aus diesen folgt, dass Browser- oder Headerinformationen, die zwangsläufig oder auf Grund der Einstellungen des Endgerätes beim Aufruf eines Telemediendienstes übermittelt werden, nicht als „Zugriff auf Informationen, die bereits in einem Endgerät gespeichert sind" angesehen werden sollen.

5. Unverhältnismäßige Folgen für die Medienfreiheit zu befürchten

Der aus den Leitlinien folgende Einwilligungs- und Rechtfertigungsvorbehalt begründet darüber hinaus einen unverhältnismäßigen Eingriff in die gemäß Art. 11 der Charta der Europäischen Grundrechte geschützte und bei der Auslegung des Art. 5 Abs. 3 ePD zu berücksichtigende Meinungs- und Informationsfreiheit.

[1] Vgl. www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

Nach Art. 11 Abs. 2 sind die Freiheit der Medien und die Pluralität zu achten. Außerdem ist das Recht auf freie Meinungsäußerung zu wahren, was einschließt, dass Informationen und Ideen ohne behördlichen Eingriff empfangen und weitergegeben werden können.

Dem läuft die weite Auslegung des Art. 5 (3) ePD für die elektronische Kommunikation diametral entgegen, wenn – wie dargelegt – angenommen werden muss, dass die Verbreitung von privaten audio-visuellen Medieninhalten bspw. im Internet grundsätzlich von der Einwilligung des Nutzers in jeden einzelnen Verbindungsvorgang abhängig gemacht wird.

Darüber hinaus entsteht durch die Auslegung eine die Medienfreiheit gefährdende behördliche Kontrollmöglichkeit über die Frage, welche Audio- und Videoinhalte etwa auf einer Webseite bei Nichteinholung einer Nutzereinwilligung noch „unbedingt erforderlich" für die Inanspruchnahme des Dienstes i. S. der nach Art. 5 Abs. 3 Satz 2 ePD vorgesehenen Ausnahme vom Einwilligungserfordernis sind. Es steht außer Frage, dass behördliche Bewertungen dieser Art die freie Verbreitung von Medieninhalten und Meinungen nachhaltig gefährden können.

Bei der Auslegung sollte schließlich stärker als bislang beachtet werden, dass datenbasierte Werbung und Marketing essenzielle Bausteine zur Finanzierung freier Medien und damit Grundlage für den Erhalt von Medienvielfalt und Medienfreiheit in Europa sind. Dies gilt umso mehr, als das die Refinanzierung privater Medien vor erheblichen Herausforderungen steht. Dies nicht nur auf Grund geänderter Nutzungsgewohnheiten, sondern insbesondere auf Grund des Wettbewerbs mit global aktiven Big-Tech-Plattformen, die das Online-Werbeumfeld dominieren und den Großteil der Werbeerlöse für sich beanspruchen. Eine Auslegung, die in dieser Marktsituation, wie vorliegend, weitere und innovationshemmende Hürden für die Verbreitung elektronischer Medien und die Ausspielung datenbasierter Werbung aufstellt, sollte besonders kritisch hinterfragt und auf ihre Medienverträglichkeit hin analysiert werden.