



Stellungnahme

des Deutschen Anwaltvereins vorbereitet durch
den Ausschuss Informationsrecht

zur Sondierung der Europäischen Kommission zu Omnibusvorschriften für den Digitalbereich (Vereinfachungspaket für den Digitalbereich)

Stellungnahme Nr.: 68/2025

Brüssel, im Oktober 2025

Mitglieder des Ausschusses

- Rechtsanwalt Prof Niko Härting, Berlin (Vorsitzender und Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierehoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski, Geschäftsführerin, Berlin

Ansprechpartner in Brüssel:

- Rechtsanwältin Dorothee Wildt, LL.M., stellv. Leitung
- Myra Jockisch, LL.M., Referentin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

I. **Alignment zwischen DSGVO und E-Privacy im Hinblick auf die Cookie-Banner beim Webtracking**

a.) **Problem**

Das Webtracking, insbesondere im Zusammenhang mit personalisierter Werbung, sollte einheitlich in der DSGVO reguliert werden. Art. 5 Abs. 3 E-Privacy-Richtlinie sollte insoweit vereinfacht werden¹.

Datenschutzrechtlich bedarf das Webtracking einer Rechtfertigung nach Art. 6 DSGVO. Denn zur Erfassung des Verhaltens eines Internetnutzers ist die Verarbeitung personenbezogener Daten notwendig. Nach Art. 6 Abs. 1 Satz 1 lit. a DSGVO stellt die Einwilligung *eine von mehreren Rechtfertigungsgründen* dar. Neben einer Einwilligung kommt insbesondere eine Rechtfertigung aufgrund berechtigter Interessen nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO in Betracht.

Art. 5 Abs. 3 E-Privacy-Richtlinie verlangt demgegenüber stets eine Einwilligung als *einzigen Rechtfertigungsgrund*. Eine Ausnahme gilt lediglich, wenn der alleinige Zweck eines gesetzten Cookies die Durchführung oder Erleichterung der Übertragung einer Nachricht ist. Die Alternativlosigkeit der Einwilligung nach Art. 5 Abs. 3 E-Privacy-Richtlinie hat dazu geführt, dass Cookie-Banner im Netz allgegenwärtig sind. Dies wird von Internetnutzern vielfach als lästig empfunden².

¹ Vgl. bereits Stellungnahme des DAV 29-17 zum Entwurf einer E-Privacy-Verordnung, Seite 11: „Insbesondere sollte geprüft werden, ob für die Verarbeitung von Kommunikationsdaten flexible Erlaubnistatbestände analog Art. 6 Abs. 1 lit. b und lit. f DSGVO ergänzt werden können (Verarbeitung zur Vertragserfüllung sowie auf Basis legitimer Interessen bei gleichzeitiger Interessenabwägung).

² Eine Befragung kam kürzlich zu dem Ergebnis, dass 51 Prozent aller Befragten manche Dienste nicht nutzen, da zu viele Cookies vorhanden sind, zuletzt abgerufen am 2.10.2025 unter <https://www.bitkom.org/Presse/Presseinformation/Drei-Viertel-von-Cookie-Bannern-genervt>; Specht-Riemenschneider/Groß/Schneider in der FAZ, zuletzt abgerufen am 7.10.2025 unter <https://www.faz.net/einspruch/so-denken-die-deutschen-wirklich-ueber-datenschutz-110712557.html>

b.) Vorschlag

Es wird daher vorgeschlagen, Art. 5 E-Privacy-Richtlinie durch einen neuen Absatz 4 zu ergänzen, der den Vorrang der DSGVO klarstellt:

- (4) ***Absatz 3 gilt nicht, soweit bei der Speicherung von Informationen oder dem Zugriff auf Informationen personenbezogene Daten der Nutzenden verarbeitet werden und daher Artikel 6 der Verordnung 2016/679 Anwendung findet.***

Soweit der alleinige Zweck eines gesetzten Cookies die Durchführung oder Erleichterung der Übertragung einer Nachricht ist, bedarf es in Art. 6 DSGVO keiner gesonderten Regelung, da in diesen Fällen die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO zu denselben Ergebnissen führen wird wie Art. 5 Abs. 3 E-Privacy-Richtlinie.

II. Meldepflicht nach Art. 33 DSGVO

a.) Problem

Erst ein mittleres Risiko sollte eine Meldepflicht begründen, da derzeit auch Geringfügigkeiten gemeldet werden müssen.

Die aktuelle Fassung von Art. 33 DSGVO verpflichtet zur Meldung jeder Verletzung des Schutzes personenbezogener Daten, sofern „ein Risiko für die Rechte und Freiheiten natürlicher Personen“ nicht ausgeschlossen werden kann. Diese niedrige Schwelle führt zu einer Flut von Meldungen, von denen ein erheblicher Teil Fälle ohne tatsächliche Relevanz für das reale Schutzniveau der personenbezogenen Daten in den Mitgliedstaaten ist. Die Datenschutzbehörden werden dadurch stark belastet und können sich weniger auf gravierende Vorfälle konzentrieren.

Sinn und Zweck der Meldepflicht ist es, Datenschutzverletzungen mit echtem Risiko für Betroffene zu erfassen und angemessen zu adressieren. Diese Fälle sollen zur Kenntnis der Aufsichtsbehörden gelangen, damit diese spezial- und generalpräventiv daran anknüpfen und das Schutzniveau individuell und strukturell anheben können. Durch die derzeitige Regelung belasten jedoch Bagatellen die Ressourcen der Aufsichtsbehörden und die internen Strukturen der Verantwortlichen. Die Effektivität der Aufsicht leidet, da Ressourcen gebunden werden, ohne dass tatsächlich die Rechte der Betroffenen geschützt werden.

Eine Meldepflicht sollte erst dann entstehen, wenn ein zumindest mittleres Risiko für die Rechte der Betroffenen vorliegt. Hier kann sich die Reform am alten § 42a BDSG orientieren, der ein „schwerwiegendes Risiko“ (konkret: drohende schwerwiegende Beeinträchtigungen) voraussetzte. Nur dann ist eine staatliche Aufsicht sinnvoll und verhältnismäßig. Im Ergebnis würde dadurch auch die in Art. 33 verfolgte Zielsetzung – effektiver Schutz bei tatsächlicher Gefährdung – erreicht und die Überlastung der Behörden vermieden.

b.) Vorschlag:

Art. 33 DSGVO sollte dahingehend geändert werden, dass eine Meldepflicht erst bei einem mindestens mittleren Risiko für die Rechte oder schutzwürdigen Interessen der Betroffenen eintritt. So werden Ressourcen auf echte Gefährdungen gelenkt und die Effektivität des Datenschutzes insgesamt gestärkt. Konkret könnte Art. 33 Abs. 1 Satz 1 DSGVO wie folgt gefasst werden:

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass soweit die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem schwerwiegenden Risiko für die Rechte und Freiheiten natürlicher Personen führt.

III. Alignment zwischen Art. 6 DSGVO und AI Act

a.) Problem

Es sollte zudem klargestellt werden, dass die Verarbeitung von personenbezogenen Daten zur Erfüllung der im AI Act normierten Pflichten als Fall einer rechtlichen Verpflichtung im Sinne von Artikel 6 Abs. 1 Satz 1 lit. c DSGVO als einschlägige Rechtsgrundlage anerkannt wird. Nur so lassen sich Wertungswidersprüche zwischen dem AI Act und der DSGVO vermeiden.

Die Pflichten aus dem AI Act stellen mittelbar auch eine Pflicht zu einer Datenverarbeitung dar. So muss beispielsweise von Anwendern geprüft werden, ob eine Hochrisiko-Anwendungsfall vorliegt und folglich ein Quality Risk Management System im Sinne des Art. 17 AI Act erstellt werden muss. Ob hierfür auch eine

datenschutzrechtliche Rechtsgrundlage besteht, ist nach geltendem Recht fraglich. Diese Unsicherheit führt zu Rechtsunsicherheit für Anbieter und Betreiber von KI-Systemen und kann die effektive Umsetzung der im AI Act vorgesehenen Regeln beeinträchtigen.

b.) Vorschlag

Es wird vorgeschlagen, Art. 6 Abs. 1 Satz 1 lt. c DSGVO, wie folgt, zu ergänzen:

*c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; **dies gilt insbesondere für die Erfüllung von Verpflichtungen nach der Verordnung (EU) 2024/1689.***

IV. Alignment zwischen Art. 9 DSGVO und AI Act

a.) Problem

Ein zentrales Anliegen des AI Acts ist die Verhinderung von Bias und Diskriminierung vulnerabler Gruppen durch KI-Systeme. Um solche Verzerrungen zu erkennen und zu beheben, ist eine Datenverarbeitung erforderlich. Insbesondere in Fällen von besonders vulnerablen Gruppen unterliegen die zu verarbeitenden Daten den besonderen Anforderungen des Art. 9 DSGVO (besondere Kategorien personenbezogener Daten). Um dieses Hindernis zu lösen, sieht Art. 10 Abs. 5 AI Act vor, dass Anbieter von KI-Systemen für die Erkennung und Korrektur von schädlichen Verzerrungen Art. 9 DSGVO Daten verarbeiten dürfen. Diese Freistellung greift jedoch insoweit zu kurz, als sie verkennt, dass nicht nur bei der Entwicklung von KI-Systemen eine Erkennung und Korrektur regelmäßig erforderlich ist, sondern auch während der Verwendung des jeweiligen KI-Systems. Um die Umsetzung der Ziele des AI-Acts zu gewährleisten, muss die Freistellung konsequenterweise auch für Betreiber von KI-Systemen gelten.

b.) Vorschlag:

Art. 10 Abs. 5 S. 1 AI Act sollte, wie folgt, ergänzt werden:

*(5) Soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen im Einklang mit Absatz 2 Buchstaben f und g dieses Artikels unbedingt erforderlich ist, dürfen die Anbieter **und Betreiber** solcher Systeme ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, wobei*

sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen.

Verteiler

Europa

Europäische Kommission

- Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CNECT)
- Generaldirektion Justiz und Verbraucher (DG JUST)

Europäisches Parlament

- Rechtsausschuss (JURI)
- Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO)
- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE)

Rat der Europäischen Union

Ständige Vertretung der Bundesrepublik Deutschland bei der EU

Justizreferenten der Landesvertretungen bei der EU

Rat der Europäischen Anwaltschaften (CCBE)

Bundesverband der Freien Berufe (BFB) – Büro Brüssel

Deutsche Industrie- und Handelskammer (DIHK) – Büro Brüssel

Bundesverband der deutschen Industrie e.V. (BDI) – Büro Brüssel