„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

2 / 2026
Februar 2026

Die KI-VO im Omnibus

Die Europäische Kommission hat einen Änderungsvorschlag für die KI-VO vorgelegt

Von Philipp Schöbel, Berlin

Die Europäische Kommission will in einem sogenannten Omnibus die europäische Digitalregulierung vereinfachen.[1] Von den geplanten Änderungen ist auch die KI-Verordnung (KI-VO)[2] betroffen. Bisher gelten zwar noch nicht alle Regelungen dieser Verordnung,[3] die EU-Kommission sieht dennoch bereits Änderungsbedarf. Durch administrative Vereinfachungen sollen Unternehmen zukünftig Milliarden einsparen können. Im Folgenden werden die wichtigsten Änderungsvorschläge vorgestellt.

I. Weniger KI-Kompetenz

Die Anforderungen an die KI-Kompetenz (Art. 4 KI-VO)[4] werden gesenkt. Anbieter und Betreiber sollen keine Maßnahmen zur Förderung der KI-Kompetenz ihres Personals mehr ergreifen müssen. Die EU-Kommission und die Mitgliedstaaten sollen Anbieter und Betreiber zukünftig nur noch dazu „ermutigen". Unklar ist, welcher Mehrwert damit verbunden wäre.

II. KI-Training und Datenschutz

Grundsätzlich berührt die KI-VO nicht die Datenschutz-Grundverordnung (DSGVO), die ePrivacy-Richtlinie und die Richtlinie zum Datenschutz in Strafsachen (JI-RL) (Art. 2 Abs. 7 S. 2 KI-VO).

Von diesem Grundsatz gibt es zwei Ausnahmen. Zum einen gibt es eine datenschutzrechtliche Verarbeitungsgrundlage für die Anwendung in KI-Reallaboren[5] (Art. 59 i.V.m. Art. 2 Abs. 2 S. 2 KI-VO). Die zweite Ausnahme gilt für die Verarbeitung von Daten im Sinne des Art. 9 DSGVO (sensible personenbezogene Daten).[6] Die Verarbeitung ist dann erlaubt, wenn sie für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist (Art. 10 Abs. 5 S. 1 i.V.m. Art. 2 Abs. 7 S. 2 KI-VO). Es handelt sich um eine Rechtsgrundlage im Sinne des Art. 9 Abs. 2 lit. g DSGVO.[7] Die Vorschrift existiert, weil diskriminierende Verzerrungen nicht immer mittels synthetischer oder anonymisierter Daten effektiv erkannt und korrigiert werden können.[8] An die Verarbeitung sind strenge Voraussetzungen geknüpft.

---

1 Europäische Kommission, Pressemitteilung 19. November 2025, Vereinfachung der Digitalgesetzgebung: Kommission legt Paket vor, abrufbar unter: https://germany.representation.ec.europa.eu/news/vereinfachung-der-digitalgesetzgebung-kommission-legt-paket-vor-2025-11-19_de (alle Quellen zuletzt abgerufen am 20.12.2025).

2 Zur Relevanz der KI-VO für Hochschulen siehe: Yang-Jacobi, Endlich eine Lösung für mehr KI in der Wissenschaft?, DFN-Infobrief Recht 1/2026; Schöbel, Das Recht auf Erklärung von KI-Entscheidungen – Teil 1, DFN-Infobrief Recht 10/2025, S. 8; KI-Kompetente Hochschulen, DFN-Infobrief Recht 08/2025, S. 7; AI Act – Licht der Europäischen Union, DFN-Infobrief Recht 12/2024, S. 7 f.; Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025, S. 2; Was sind Quasi-Anbieter von KI-Systemen?, DFN-Infobrief Recht 1/2026, S. 14.

3 Die KI-VO gilt ab dem 02.08.2026, Art. 113 Abs. 2 KI-VO. Einige Regelungen – wie etwa die Verbote – gelten bereits seit dem 02.02.2025, Art. 113 Abs. 2 lit. a KI-VO. Die Regelungen zu Hochrisiko-KI-Systemen gelten erst ab dem 02.08.2027, Art. 113 Abs. 3 lit. c KI-VO.

4 Siehe zur KI-Kompetenz: Schöbel, KI-Kompetente Hochschulen, DFN-Infobrief Recht 08/2025, S. 7.

5 Zu KI-Reallaboren siehe: Schöbel, Europäische Sandkästen für KI, DFN-Infobrief Recht 08/2024, S. 2.

6 Siehe zu Art. 9 DSGVO im Rahmen des KI-Trainings: Müller-Westphal, Es bleibt alles anders, DFN-Infobrief Recht 02/2026.

7 Kilian/Schefzig in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO, Art. 10 Rn. 69.

8 Kilian/Schefzig in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO, Art. 10 Rn. 59.

Der Vorschlag der Kommission will diese Regelung ausweiten. Sie soll etwa nicht nur für Anbieter, sondern auch für Betreiber von Hochrisiko-KI-Systemen gelten.

III. Neue Ausnahme der Registrierungspflicht

Anbieter, deren KI-System ein Hochrisiko-KI-System nach Art. 6 Abs. 2 i.V.m. Anhang III KI-VO darstellt, können sich möglicherweise auf eine Ausnahme nach Art. 6 Abs. 3 KI-VO berufen. Ein KI-System gilt dann nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt. Dies ist insbesondere der Fall, wenn unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst wird (Art. 6 Abs. 3 UAbs. 1 KI-VO). Dann müssen die Anbieter aber ab dem Zeitpunkt des Inkrafttretens der Regelungen zu Hochrisiko-KI-Systemen[9] ihr System in der EU-Datenbank für Hochrisiko-KI-Systeme registrieren (Art. 6 Abs. 4 S. 2 i.V.m. Art. 49 Abs. 2 KI-VO). Der Vorschlag der Kommission will diese Registrierungspflicht abschaffen. Dies hätte zur Folge, dass Anbieter von Hochrisiko-KI-Systemen, die sich auf eine Ausnahme nach Art. 6 Abs. 3 KI-VO berufen, ihr System nicht mehr in der EU-Datenbank registrieren müssten. Dies würde auch Hochschulen betreffen, die der Auffassung sind, dass ihr KI-System zwar unter Anhang III Nr. 3 fällt (allgemeine und berufliche Bildung), sie es dennoch nicht als hochriskant einstufen.

IV. Erleichterungen für KMUs und SMCs

In der KI-VO sind jetzt schon Erleichterungen für kleine und mittlere Unternehmen (KMU) vorgesehen. Zukünftig sollen auch Midcap-Unternehmen (SMC)[10] davon profitieren. Neben der klassischen Kategorie der KMU schafft die Kommission eine Kategorie für Unternehmen, die zwischen KMU und Großkonzernen angesiedelt sind. Diese kleinen SMCs wachsen oftmals schneller als KMUs und weisen einen höheren Innovationsgrad auf. Sie stehen in Bezug auf den bürokratischen Aufwand der Digitalregulierung nach Ansicht der Kommission vor ähnlichen Herausforderungen wie KMU.[11]

Der Entwurf führt neue Definitionen für KMUs (Art. 3 Nr. 14a) und SMCs (Art. 13 Nr. 14b) ein. In der KMU-Definition wird auf die Definition für KMUs aus dem Anhang zur Empfehlung der Kommission zur Definition von KMU verwiesen. Danach sind KMUs solche Unternehmen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.[12] Die Definition für SMCs verweist auf den Anhang der Empfehlung der Kommission zur Definition kleiner Midcap-Unternehmen. Danach sind SMCs solche Unternehmen, die nicht unter die Definition für KMUs fallen, die weniger als 750 Personen beschäftigen und die einen Jahresumsatz von höchstens 150 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 129 Mio. EUR beläuft.[13] Kleinere Hochschulen und Forschungseinrichtungen sollten prüfen, ob sie eventuell unter den Begriff der KMU oder SMC fallen.

1. Geldbußen

Der derzeit geltende Art. 99 der KI-VO sieht vor, dass die Mitgliedstaaten Vorschriften zur Sanktion von Verstößen gegen die KI-VO erlassen müssen. Dabei müssen sie ausdrücklich die Interessen von KMUs und deren wirtschaftliches Überleben berücksichtigen (Art. 99 Abs. 1 S. 3 KI-VO). In der aktuellen Fassung der KI-VO können Geldbußen bis zu einem Höchstbetrag oder bis zu einem bestimmten Prozentsatz des gesamten weltweiten

9 Die Regelungen des Art. 6 gelten ab dem 02.08.2027 gemäß Art. 113 Abs. 3 lit. c KI-VO.

10 Die Abkürzung ist aus der englischen Sprachfassung entlehnt, wo sie für „small mid-cap enterprise“ steht.

11 Erwägungsgrund(Erwg) 4 Proposal for a Regulation of the European Parliament and of the Council, amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 19.11.2025, COM(2025) 836 final, 2025/0359 (COD).

12 Art. 2 Anhang Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. L 124/36, v. 20.5.2003.

13 Nr. 2 Anhang Empfehlung (EU) 2025/1099 der Kommission vom 21. Mai 2025 zur Definition kleiner Midcap-Unternehmen, ABl. L vom 28.5.2025.

Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Dabei ist der jeweils höhere Betrag ausschlaggebend.[14] Für KMUs gilt, dass der jeweils niedrigere Betrag als Geldbuße zu wählen ist (Art. 99 Abs. 6 KI-VO). Der Änderungsentwurf erstreckt diese Privilegierung auch auf SMCs.

2. Technische Dokumentation

Anbieter[15] von Hochrisiko-KI-Systemen müssen nach der derzeit geltenden KI-VO eine technische Dokumentation erstellen (Art. 11 Abs. 1 i.V.m. Art. 16 lit. a KI-VO).[16] Schon jetzt ist vorgesehen, dass diese technische Dokumentation von KMUs in vereinfachter Weise bereitgestellt werden kann (Art. 11 Abs. 1 UAbs. 2 S. 3 KI-VO). Außerdem soll die Kommission bereits jetzt zu diesem Zweck ein vereinfachtes Formular für die technische Dokumentation, das auf die Bedürfnisse von KMUs zugeschnitten ist, erstellen (Art. 11 Abs. 1 UAbs. 2 S. 4 KI-VO). Der Omnibus-Vorschlag sieht vor, dass auch SMCs von dieser vereinfachten Dokumentationspflicht profitieren sollen und dass die Kommission bei der Erstellung des entsprechenden Musterformulars auch die Bedürfnisse von SMCs berücksichtigt.

3. Qualitätsmanagementsysteme

Anbieter von Hochrisiko-KI-Systemen müssen nach der derzeit geltenden KI-VO ein sogenanntes Qualitätsmanagementsystem einrichten (Art. 17 i.V.m. Art. 16 lit. c KI-VO). Dieses soll die Einhaltung der KI-VO gewährleisten (Art. 17 Abs. 1 S. 1 KI-VO). Schon jetzt soll die Umsetzung in einem angemessenen Verhältnis zur Größe der Organisation des Anbieters erfolgen (Art. 17 Abs. 2 S. 1 KI-VO). Der Omnibus-Entwurf will im Wortlaut verankern, dass dies „insbesondere" für KMUs und SMCs gelten soll.

4. Behördliche Beratung

Der derzeitige Art. 70 Abs. 8 KI-VO sieht vor, dass die zuständigen nationalen Behörden KMUs mit Anleitung und Beratung bei der Durchführung dieser Verordnung zur Seite stehen können. Der Kommissionsentwurf erstreckt diese Beratungsmöglichkeit auch auf SMCs. Der Entwurf für das deutsche KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG-E) sieht innovationsfördernde Maßnahmen vor. § 12 Nr. 1 statuiert, dass die Bundesnetzagentur allgemeine Informationen und Anleitungen zur Anwendung der KI-VO, insbesondere für KMUs sowie für Start-ups bereitstellen wird. Eine Änderung der KI-VO dürfte wohl auch eine Anpassung des KI-MIG-E in diesem Bereich nach sich ziehen.

5. Freiwillige Unterstützungsinstrumente

Schon jetzt sollen das Europäische Büro für Künstliche Intelligenz und die Mitgliedstaaten die Aufstellung von Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen fördern. Dabei geht es darum, dass die Pflichten, die für Hochrisiko-KI-Systeme gelten, auch von Anbietern anderer Systeme freiwillig angewendet werden (vgl. Art. 95 Abs. 1 KI-VO). Dabei sollen die besonderen Interessen und Bedürfnisse von KMUs berücksichtigt werden. Nach dem Omnibus-Vorschlag sollen auch die Interessen und Bedürfnisse von SMCs berücksichtigt werden.

Die Kommission muss Leitlinien für die praktische Umsetzung der KI-VO veröffentlichen (Art. 96 Abs. 1 UAbs. 1 KI-VO). Teilweise sind solche Leitlinien auch schon erschienen.[17] Schon jetzt ist festgelegt, dass sie dabei den Bedürfnissen von KMUs einschließlich Start-up-Unternehmen besondere Aufmerksamkeit widmen soll (Art. 96 Abs. 1 UAbs. 2 KI-VO). Der Omnibus-Vorschlag will diese Bestimmung auch auf SMCs ausweiten.

---

14 Vgl. Art. 99 Abs. 3-5 KI-VO.

15 Zur Frage, ob Hochschulen Anbieter oder Quasi-Anbieter von Hochrisiko-KI-Systemen sein können, siehe: Schöbel, Was sind Quasi-Anbieter von KI-Systemen?, DFN-Infobrief Recht 1/2026, S. 14.

16 Die Pflichten der Anbieter von Hochrisiko-KI-Systemen werden in einem kommenden Beitrag im Infobrief Recht ausführlich dargestellt.

17 Siehe etwa die Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), 29.07.2025, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act; oder die Leitlinien der Kommission zur Definition eines Systems der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), 29.07.2025, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.

V. Ausweitung der Innovationsförderung

Der Omnibus-Vorschlag sieht eine Ausweitung der innovationsfördernden Maßnahmen der KI-VO vor. Dazu zählen die Regelungen über KI-Reallabore (Art. 57 ff. KI-VO) und zu Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren (Art. 60 KI-VO). Zukünftig sollen KI-Reallabore auch auf EU-Ebene durch das europäische KI-Büro eingerichtet werden können. Der Anwendungsbereich der Tests und Realbedingungen soll ausgeweitet werden. Bisher gelten diese Regelungen nur für anwendungsbezogene Hochrisiko-KI-Systeme. Sie sollen zukünftig auch für produktbezogene Hochrisiko-KI-Systeme gelten.

VI. Aufschub für die Geltung der Regelungen zu Hochrisiko-KI

Die Regelungen bezüglich Hochrisiko-KI-Systemen gelten noch nicht und sollen laut dem derzeit gültigen Verordnungstext ab dem 2. August 2027 gelten (Art. 113 Abs. 3 lit. c KI-VO). Allerdings verzögert sich derzeit die Ausarbeitung technischer Normen, die die Umsetzung der Pflichten für Hochrisiko-KI-Systeme erleichtern sollen. Darüber hinaus verzögert sich auch die Einrichtung des nationalen Governance- und Konformitätsbewertungsrahmens auf der Ebene der Mitgliedstaaten. Der Complianceaufwand für betroffene Unternehmen ist nach Ansicht der Kommission höher als erwartet.[18]

Die Geltung der Pflichten für Hochrisiko-KI-Systeme soll an einen Beschluss der Kommission gekoppelt werden, der bestätigt, dass Maßnahmen zur Unterstützung der Einhaltung der Hochrisiko-KI-Pflichten (damit gemeint sind technische Normen) verfügbar sind. Die Pflichten für anwendungsbezogene Hochrisiko-KI-Systeme (Anhang III KI-VO) sollen sechs Monate nach dem Beschluss gelten. Auch wenn es keinen solchen Beschluss geben sollte, sollen sie ab dem 2. Dezember 2027 gelten. Die Pflichten für produktbezogene Hochrisiko-KI-Systeme (Anhang I KI-VO) sollen zwölf Monate nach dem Beschluss gelten. Auch wenn es keinen solchen Beschluss geben sollte, sollen sie ab dem 2. August 2028 gelten.

VII. Fazit

Daneben gibt es noch weitere Änderungsvorschläge. So sollen auch die Kompetenzen des Büros für Künstliche Intelligenz ausgeweitet werden. Außerdem sind Änderungen für die nationalen notifizierenden Behörden geplant.

Bisher handelt es sich nur um einen Vorschlag der Kommission. Nun müssen sich das Europäische Parlament und der Rat damit auseinandersetzen. Der damalige Entwurf der Kommission zur KI-VO wurde im Gesetzgebungsverfahren teilweise stark geändert. Es ist fraglich, ob die jetzt vorgeschlagenen Änderungen noch einmal grundlegend angepasst werden und welche Änderungen im Laufe des Gesetzgebungsverfahrens dazukommen.

18 Erwg. 2 COM(2025) 836 final, 2025/0359 (COD).

Alles bleibt anders

Geplante Reformen der DSGVO im Rahmen des digitalen Omnibusses

Von Johannes Müller-Westphal, Berlin

Mit ihrem sogenannten digitalen Omnibus[1] plant die Europäische Kommission eine Reform der europäischen Digitalvorschriften. Diese Reform zielt darauf ab, die Regulierung digitaler Technologien zu verschlanken und hierdurch Unternehmen zu entlasten. Hierzu sind auch Änderungen der Datenschutz-Grundverordnung (DSGVO) geplant, durch die die regulatorische Belastung für Daten verarbeitende Stellen gesenkt werden soll.

I. Digitaler Omnibus zur Vereinfachung des europäischen Digitalrechts

Am 19. November 2025 hat die Europäische Kommission im Rahmen eines „Digital Package" den sogenannten digitalen Omnibus vorgestellt. Er soll das EU-Digitalrecht, das in den letzten Jahren stark angewachsen ist, entschlacken und anwendungsfreundlicher machen. Hierbei soll aber nicht der durch die Verordnungen garantierte hohe Grundrechtsschutz für Unionsbürger aufgegeben werden. Durch den Abbau von Bürokratie und Rechtsunsicherheit sollen Unternehmen Kosten sparen können. Dadurch soll die Innovationskraft der europäischen Wirtschaft gestärkt werden.

Der digitale Omnibus wirkt sich auf verschiedene europäische Rechtsakte aus. Eine Vereinfachung des europäischen Digitalrechts soll unter anderem dadurch erfolgen, dass die Regelungen des Data Governance Act[2], der Verordnung zum freien Verkehr nichtpersonenbezogener Daten und der Open Data Directive in den Data Act[3] aufgenommen werden. Hierdurch soll ein übersichtlicher Datenrechtsakt geschaffen werden, vorgesehen sind zudem punktuelle inhaltliche Änderungen.

Ebenso betrifft der digitale Omnibus verschiedene Cybersicherheitsvorschriften der Europäischen Union. Der Vorschlag der Europäischen Kommission sieht diesbezüglich vor allem eine Harmonisierung der Meldepraxis vor. Über einen Single-Entry-Point sollen IT-Sicherheitsvorfälle zentral gemeldet und so die Anforderungen aus verschiedenen Rechtsakten gebündelt erfüllt werden können.

Auch die KI-VO ist vom digitalen Omnibus betroffen. Die Europäische Kommission koppelt dabei insbesondere zentrale Pflichten aus der KI-VO an die Verfügbarkeit der hierfür erforderlichen Standards, Leitlinien und Unterstützungsinstrumente. Zudem werden Erleichterungen für kleine und mittlere Unternehmen erweitert.

Verschiedene inhaltliche Änderungen sieht der digitale Omnibus auch für die DSGVO vor.

II. Änderungen der DSGVO

Nachfolgend sollen einige der wesentlichen Änderungen, die von der Kommission für die DSGVO vorgeschlagen sind, dargestellt werden.

---

1 Der Entwurf ist in englischer Sprache unter folgendem Link abrufbar https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-regulation-proposal (alle Links dieses Beitrags zuletzt abgerufen am 11.12.2025).

2 Zum Data Governance Act, Müller, Geteiltes Wissen ist doppeltes Wissen, DFN-Infobrief Recht 01/2024.

3 Zum Data Act, Müller, Die Daten sind frei?, DFN-Infobrief Recht 03/2024.

1. Begriff der personenbezogenen Daten

Zentral für die Anwendung der DSGVO ist der Begriff der personenbezogenen Daten. Dieser wird in Art. 4 Nr. 1 DSGVO definiert. Hiernach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Reformvorschlag sieht vor, dass diese Definition durch die Klarstellung ergänzt wird, dass nicht zwingend personenbezogene Daten vorliegen, wenn eine spezifische Person oder Einrichtung über die jeweiligen Informationen verfügt, aber nur eine andere Person oder Einrichtung imstande ist, die betroffene Person zu identifizieren. Sofern die Stelle, die über die Daten verfügt, nicht selbst imstande ist, die betroffene Person mit den Mitteln zu identifizieren, über die sie vernünftigerweise verfügt, soll für die Stelle kein personenbezogenes Datum vorliegen. Damit würde die Definition von personenbezogenen Daten an die Rechtsprechung des Europäischen Gerichtshofs (EuGH) angeglichen werden. Dieser vertritt bereits einen relativen Ansatz, um festzustellen, ob ein personenbezogenes Datum vorliegt. Hiernach muss gefragt werden, ob der jeweilige Verantwortliche imstande ist, die betroffene Person mit verhältnismäßigen Mitteln zu identifizieren.[4] In seinem Urteil vom 4. September 2025 (Az. C-413/23 P Rn. 68 ff) hat der EuGH diese Rechtsprechung erneut bestätigt und ausgeführt, dass für eine bestimmte Stelle kein Personenbezug vorliegt, obwohl andere Einrichtungen imstande wären, die betroffene Person zu identifizieren. Diese Rechtsprechung würde durch die Reform bestätigt und weiter verfestigt werden.

2. Zweckbindungsgrundsatz

Der Zweckbindungsgrundsatz zählt zu den Kernelementen des Datenschutzrechts. Er ist in Art. 5 Abs. 1 lit. b DSGVO normiert. Hiernach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Vorschrift führt weiter aus, dass eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke in Übereinstimmung mit Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Eine weitere Hilfe gibt Art. 6 Abs. 4 DSGVO, der einige Kriterien nennt, anhand derer geprüft werden kann, ob der neue Verarbeitungszweck mit dem ursprünglichen Zweck vereinbar ist, zu dem die Daten erhoben wurden. Der Reformvorschlag des digitalen Omnibusses sieht eine leichte Änderung in der Formulierung von Art. 5 Abs. 1 lit. b DSGVO vor. Demnach sollen Verarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken in Übereinstimmung mit Art. 89 DSGVO als vereinbar mit den ursprünglichen Zwecken gelten. Diese Vereinbarkeit soll unabhängig von Art. 6 Abs. 4 DSGVO vorliegen. Es muss also nicht geprüft werden, ob die genannten Kriterien vorliegen. Diese Änderung kann Datenverarbeitungen zu Forschungszwecken erleichtern. Häufig werden hierfür Daten genutzt, die für andere Zwecke erhoben wurden, sodass der Zweckbindungsgrundsatz einer Weiterverarbeitung zu Forschungszwecken entgegenstehen könnte. Der neue Vorschlag nimmt hingegen pauschal an, dass die Datenverarbeitung zu Forschungszwecken nicht gegen den Zweckbindungsgrundsatz verstößt, sofern die in Art. 89 DSGVO vorgesehenen besonderen Garantien eingehalten werden. Damit würden Datenverarbeitungen zu Forschungszwecken eine deutliche Privilegierung erfahren.

3. Verarbeitung besonders sensibler Daten zum Zweck des KI-Trainings

Für besonders sensible Datenkategorien (etwa Gesundheitsdaten) sieht die DSGVO in Art. 9 erhöhte Verarbeitungsanforderungen vor. Im Gegensatz zu Art. 6 DSGVO, der die Verarbeitungsbedingungen für sonstige personenbezogene Daten normiert, sieht Art. 9 DSGVO nicht die Möglichkeit vor, dass die besonders sensiblen Daten auch aufgrund eines überwiegenden berechtigten Interesses der Daten verarbeitenden Stelle verarbeitet werden dürfen. Damit ist es in vielen Fällen zwingend erforderlich, eine Einwilligung der betroffenen Person einzuholen, um besonders sensible personenbezogene Daten zu verarbeiten. In der letzten Zeit wurde insbesondere intensiv diskutiert, ob Art. 9 DSGVO der Verarbeitung personenbezogener Daten zu KI-Trainingszwecken entgegensteht.[5] Im Rahmen des Trainings von KI-Modellen kann häufig nicht ausgeschlossen werden, dass auch sensible personenbezogene Daten verarbeitet werden. Der digitale Omnibus sieht nun vor, dass die Verarbeitung besonders sensibler personenbezogener Daten im Zusammenhang

4 Hierzu Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 01/2024.

5 Müller-Westphal, Ohne Widerspruch ist alles erlaubt, DFN-Infobrief Recht 10/2025.

mit der Entwicklung und dem Betrieb eines KI-Systems unter bestimmten Bedingungen zulässig sein soll. Diese zusätzlichen Bedingungen sehen vor, dass der Verantwortliche technische und organisatorische Maßnahmen ergreifen soll, um die Erhebung und Verarbeitung besonders sensibler Daten zu vermeiden. Sofern der Verantwortliche trotzdem feststellt, dass besonders sensible Daten in den Trainingsdaten oder im KI-System selbst enthalten sind, muss er diese Daten entfernen. Sofern für die Entfernung ein unverhältnismäßiger Aufwand erforderlich ist, muss der Verantwortliche jedenfalls unverzüglich sicherstellen, dass die Daten vom KI-Modell nicht ausgegeben werden können. Werden personenbezogene Daten, die nicht als besonders sensibel gelten und nicht unter Art. 9 DSGVO fallen, zum KI-Training verarbeitet, soll sich der Verantwortliche auf den Erlaubnistatbestand des überwiegenden berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO berufen können. Dies soll ein neu eingefügter Art. 88c DSGVO klarstellen. Gleichzeitig führt dieser Artikel aber auch aus, dass der Verantwortliche angemessene technische und organisatorische Maßnahmen zu ergreifen hat, um insbesondere eine Offenlegung der personenbezogenen Daten zu verhindern.

4. Informationspflichten

Sofern ein Verantwortlicher personenbezogene Daten verarbeiten möchte, muss er die betroffene Person hierüber informieren. Erhebt der Verantwortliche selbst die Daten, muss er der Informationspflicht gemäß Art. 13 DSGVO zum Zeitpunkt der Datenerhebung nachkommen. Er muss der betroffenen Person unter anderem seinen Namen, seine Kontaktdaten und den Zweck der Datenverarbeitung mitteilen. Momentan sieht Art. 13 Abs. 4 DSGVO vor, dass die Informationspflicht lediglich dann entfällt, wenn die betroffene Person bereits über die Informationen verfügt. Diese Ausnahme soll erweitert werden. Demnach soll die Informationspflicht auch entfallen, wenn die Daten im Rahmen einer klaren und begrenzten Beziehung erhoben werden und der Verantwortliche keine verarbeitungsintensiven Tätigkeiten ausübt. Gleichzeitig muss man davon ausgehen können, dass die betroffene Person bereits über die Informationen verfügt. Anders als in der derzeitigen Fassung ist es aber nicht erforderlich, dass tatsächlich feststeht, dass die betroffene Person über die Informationen verfügt. Die Erwägungsgründe nennen als Beispiel für einen Anwendungsfall der neu geplanten Ausnahmevorschrift unter anderem Anstellungsverhältnisse. Hier könnte eine erhebliche Entlastung für die Verwaltung von Hochschulen entstehen. Diese müssten ihre Beschäftigten und möglicherweise auch ihre Studierenden nicht über jede kleinteilige Datenverarbeitung informieren, sofern davon ausgegangen werden kann, dass die betroffenen Personen über die Informationen verfügen.

Darüber hinaus soll eine weitere Ausnahme für Datenverarbeitungen zu Forschungszwecken eingefügt werden. Sofern die zusätzlichen Garantien in Art. 89 Abs. 1 DSGVO eingehalten werden, kann die Informationspflicht bei Datenverarbeitungen zu Forschungszwecken entfallen, wenn eine Erfüllung der Informationspflicht unmöglich oder mit unverhältnismäßigem Aufwand verbunden wäre. Ebenso soll die Pflicht entfallen, wenn durch die Informationspflicht das Erreichen der Verarbeitungsziele unmöglich oder ernsthaft beeinträchtigt werden würde. Mit dieser Änderung würde Art. 13 DSGVO hinsichtlich Datenverarbeitungen zu Forschungszwecken an Art. 14 DSGVO angeglichen werden. Art. 14 DSGVO normiert die Informationspflicht in der Konstellation, dass der Verantwortliche personenbezogene Daten verarbeitet, die er nicht selbst erhoben hat, oder dass er die selbst erhobenen Daten zu einem neuen Zweck weiterverarbeitet. Hier sieht bereits das geltende Recht in Art. 14 Abs. 5 lit. b DSGVO eine Ausnahme der Informationspflicht, insbesondere für Archiv-, Forschungs- und statistische Zwecke, vor, sofern eine Erfüllung der Pflicht unmöglich wäre oder einen unverhältnismäßigen Aufwand erfordert.

5. Cookies

Zudem soll die DSGVO zukünftig auch Regelungen zu Cookies beinhalten. Zuvor fielen Regelungen hierzu in den Anwendungsbereich der ePrivacy-Richtlinie. Die Kommission plant nun die Aufnahme neuer Regelungen in Art. 88a und Art. 88b DSGVO. Art. 88a DSGVO übernimmt einige Kernelemente des bereits geltenden Rechts und modifiziert sie in eine nutzerfreundlichere Form. Als Grundprinzip sieht Art. 88a DSGVO vor, dass der Zugriff auf Informationen in dem Endgerät einer natürlichen Person oder das Speichern entsprechender Informationen grundsätzlich nur mit Einwilligung der Person zulässig ist. Spezifische, in der Regel technisch bedingte Verarbeitungen werden hiervon ausgenommen. Neu ist eine explizite Regelung zur Verhinderung sogenannter Consent Fatigue, die bei Internetnutzern durch die ständige Konfrontation mit Cookie- und Einwilligungsbannern auftreten kann. Hierzu sieht der geplante Art. 88a Abs. 4 DSGVO vor, dass Nutzer eine Einwilligungsaufforderung mit einem einzelnen Klick ablehnen können müssen. Sofern Nutzer ihre Einwilligung erklärt haben, sollen sie nicht erneut um Zustimmung

gebeten werden. Haben sie die Einwilligungsaufforderung abgelehnt, dürfen sie nicht innerhalb von sechs Monaten erneut um ihre Zustimmung gebeten werden.

Eine weitere Ergänzung ist in Art. 88b DSGVO vorgesehen, der Regelungen zu einer neuen Infrastruktur für standardisierte, automatisierte Cookie-Einwilligungen vorsieht. Über diese Infrastruktur sollen insbesondere Browser automatisiert Einwilligungen oder Ablehnungen an Websites übermitteln. So sollen Nutzer idealerweise einmalig im Browser ihre Präferenzen in Bezug auf Cookies angeben können. Diese soll der Browser dann automatisiert den besuchten Websites mitteilen. Verantwortliche Websitebetreiber werden durch Art. 88b DSGVO verpflichtet, eine solche automatisierte Einwilligung oder Ablehnung von Cookies zu akzeptieren. Ebenso werden große Unternehmen, die Browser anbieten, verpflichtet, entsprechende technische Einstellungen vorzunehmen, die automatisierte Cookie-Einwilligungen und -ablehnungen ermöglichen.

III. Ausblick

Der digitale Omnibus in seiner aktuellen Fassung stellt derzeit nur einen Reformvorschlag der Europäischen Kommission dar. Dieser Gesetzesentwurf muss nun vom Europäischen Parlament und dem Rat der EU akzeptiert werden. Hierbei können die Gremien auch jeweils weitere Änderungen vorschlagen, die aber ebenfalls der Zustimmung beider Organe benötigen. Häufig findet im Gesetzgebungsprozess ein Trilog zwischen Kommission, Parlament und Rat statt. Bei diesem informellen Verfahren kommen Vertreter der Organe zusammen und versuchen, eine vorläufige Einigung zum Gesetzesvorhaben zu finden, das die Zustimmung aller Organe findet.
Im Rahmen dieses weiteren Gesetzgebungsprozesses ist es nicht unwahrscheinlich, dass sich die Reform der DSGVO noch inhaltlich ändert. Der aktuelle Reformvorschlag sieht sich bereits einiger Kritik ausgesetzt. Insbesondere fürchten Nichtregierungsorganisationen, die sich der Durchsetzung des Datenschutzrechts verschrieben haben, eine erhebliche Absenkung des derzeitigen Datenschutzstandards.[6] Im Rahmen des weiteren Gesetzgebungsvorhabens werden die verschiedenen Interessensgruppen sich bemühen, bei den europäischen Entscheidungsträgern Gehör zu finden.

IV. Relevanz für wissenschaftliche Einrichtungen

Die von der Kommission geplanten Reformen der DSGVO würden auch mit Erleichterungen für wissenschaftliche Einrichtungen einhergehen, die personenbezogene Daten verarbeiten. Datenverarbeitungen zu Forschungszwecken sollen durch die Reform weiter privilegiert werden. Insbesondere soll die Weiterverarbeitung personenbezogener Daten zu Forschungszwecken bei Einhaltung von Schutzgarantien nicht gegen den Zweckbindungsgrundsatz verstoßen. Dies würde eine erhebliche Erleichterung für die Forschung mit personenbezogenen Daten bedeuten, da Wissenschaftler so auch ohne jeden rechtlichen Zweifel Datensätze verwenden könnten, die für andere Zwecke erhoben wurden.

Sofern wissenschaftliche Einrichtungen eigene KI-Modelle entwickeln, würden sie ebenso von den geplanten Privilegierungen für Datenverarbeitungen zum Zweck der KI-Entwicklung profitieren.

6 Vgl. etwa die Analyse der NGO nyob, abrufbar unter https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf oder der Kommentar von netzpolitik.org, abrufbar unter https://netzpolitik.org/2025/digitaler-omnibus-auf-crash-kurs-mit-digitalen-grundrechten/.

Anonym oder pseudonym? Alles ist möglich.

Der Europäische Gerichtshof hat zum Verständnis des Begriffs „personenbezogene Daten“ entschieden

Von Anna Maria Yang-Jacobi, Berlin

Was sind „personenbezogene Daten“ nach europäischem Datenschutzrecht? Diese Frage beantwortete der Europäische Gerichtshof (EuGH) im September 2025.[1] Somit herrscht in einem langjährigen Streit endlich Rechtsklarheit.[2] Viele anschließende Fragen bleiben jedoch offen. Auch Hochschulen und Forschungseinrichtungen sollten sich mit dem Urteil befassen. Das Urteil kann viele Auswirkungen haben. So könnte sich dadurch eine Chance für Forschungsprojekte und das Training von Künstlicher Intelligenz (KI) bieten.

I. Generell: personenbezogene Daten vs. anonyme Daten

Nach Art. 1 Abs. 1 der Datenschutzgrundverordnung (DSGVO)[3] schützen die Vorschriften der DSGVO natürliche Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr solcher Daten. Die Regelungen der DSGVO sind also grundsätzlich nur anwendbar, wenn es sich um personenbezogene Daten natürlicher Personen handelt. Daten, die keinen Personenbezug aufweisen, sind entsprechend nicht vom Anwendungsbereich der DSGVO umfasst. In vielen Fällen ist es leicht zu beantworten, ob Daten einen Personenbezug haben. Sogenannte direkte Identifikationsmerkmale wie der Name, die Anschrift, das Geburtsdatum oder auch äußerliche Merkmale wie Geschlecht, Augenfarbe, Größe und Gewicht sind eindeutig personenbezogene Daten.[4] Daten können allerdings auch pseudonymisiert und sogar anonymisiert werden.

1. Pseudonymisierung

Die Pseudonymisierung ist eine technische Maßnahme zum Schutz personenbezogener Daten. Die betroffene Person selbst, ein Dritter oder auch ein Verantwortlicher können personenbezogene Daten so umwandeln, dass die betroffene Person nur über weitere Informationen identifizierbar ist. Es gibt verschiedene technische Möglichkeiten, um direkte Identifikationsmerkmale zum Beispiel durch einen Code, Ziffern, Zahlenabfolgen oder andere Pseudonyme zu ersetzen. In einem weiteren Schritt müssen die Daten organisatorisch durch angemessene Schutzmaßnahmen gesichert werden. Sofern eine Daten verarbeitende Stelle allerdings über die zusätzlichen Informationen verfügt, kann sie den Personenbezug problemlos wiederherstellen und eine Re-Identifizierung durchführen. In solchen Fällen ändert sich der Personenbezug der Daten folglich nicht. Die Daten bleiben trotz Pseudonymisierung weiterhin personenbezogene Daten, was auch Erwägungsgrund (ErwGr) 26 Satz 2 DSGVO aufzeigt. Art. 4 Nr. 5 DSGVO enthält eine Legaldefinition der „Pseudonymisierung“.

1 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P.

2 Zur Entscheidung der Vorinstanz und der Unterscheidung des relativen und absoluten Verständnisses bereits ausführlich Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.

3 Verordnung (EU) 2016/679.

4 Vgl. die Aufzählung von Schild, in: BeckOK Datenschutzrecht, 53. Edition, Stand: 1.8.2025, DSGVO Art. 4 Rn. 3 sowie Rn. 16.

2. Anonymisierung

Im Gegensatz dazu enthält die DSGVO weder eine Definition der „Anonymisierung“ noch Ausführungen zu speziellen Anonymisierungsverfahren. Anonyme Informationen bzw. Daten werden nur in ErwGr 26 Satz 5 und 6 DSGVO erwähnt. Allgemein beschreibt die Anonymisierung im Rahmen des Datenschutzrechts einen Vorgang, der den Personenbezug so von den Daten trennt, dass nach dem datenschutzrechtlichen Verständnis für den Verantwortlichen kein verhältnismäßiges Mittel zur Verfügung steht,[5] diese Daten eindeutig einer individuell bestimmbaren Person zuzuordnen. Anonyme Daten weisen entsprechend keinen Personenbezug auf. Die DSGVO findet nach ErwGr 26 Satz 6 DSGVO bei anonymen Daten keine Anwendung. Aus technischer Sicht gibt es verschiedene Verfahren der Anonymisierung, die auch kombiniert werden können.[6] Gerade mit Blick auf technische Weiterentwicklungen ändern sich auch die Anforderungen, die an eine Anonymisierung zu stellen sind.[7] Dabei ist eine vollständige Anonymisierung von personenbezogenen Daten aus technischer Sicht anzuzweifeln.[8]

II. SRB-Urteil des EuGH

Hintergrund des Rechtsstreits vor dem EuGH waren Datenverarbeitungen bei der Abwicklung einer spanischen Bank. Finanzbehörden wickeln ein Finanzinstitut ab, wenn es ausfällt oder ein Ausfall wahrscheinlich ist und die Stabilität des Finanzsektors gewährleistet werden soll. Ein Ausfall liegt beispielsweise vor, wenn eine Bank ihre Schulden nicht mehr begleichen kann oder die Bank die gesetzlichen Zulassungsanforderungen nicht mehr erfüllt. Bei großen europäischen Finanzinstituten ist eine europäische Behörde für die ordnungsgemäße Abwicklung zuständig: der sogenannte Einheitliche Abwicklungsausschuss (engl.: Single Resolution Board, kurz: SRB). 2018 erhob der SRB in einem ersten Verfahrensschritt persönliche Daten von Anteilshabenden und Kreditgebenden (nachfolgend: betroffene Personen/Betroffenen) der ausfallenden spanischen Bank. Der SRB veröffentlichte auf seiner Webseite eine Datenschutzerklärung, um über die Datenverarbeitung zu informieren. In einem zweiten Schritt sollten die Betroffenen Stellungnahmen abgeben. Der SRB verarbeitete die persönlichen Daten und die Stellungnahmen getrennt voneinander. Um eine spätere interne Zuordnung zu ermöglichen, erhielten die Stellungnahmen eine 33-stellige, zufällig generierte Identifikationsnummer. Diese Stellungnahmen inklusive Identifikationsnummer übermittelte der SRB zur weiteren Bewertung an die Wirtschaftsprüfungsgesellschaft Deloitte. Über diese mögliche Übermittlung an Deloitte informierte der SRB die Betroffenen in seiner Datenschutzerklärung nicht. Der Datenempfänger, Deloitte, hatte zu keinem Zeitpunkt Zugang zu den persönlichen Daten des ersten Schritts.[9] 2019 erreichten den Europäischen Datenschutzbeauftragten (EDSB) Beschwerden von Betroffenen. Der EDSB entschied daraufhin, dass es sich bei den vom SRB übermittelten Daten um personenbezogene Daten handelte und der SRB gegen das europäische Datenschutzrecht verstoßen habe. Die Betroffenen hätten darüber informiert werden müssen, dass ihre personenbezogenen Daten an Dritte übermittelt werden. Nach einem erfolglosen Überprüfungsverfahren klagte der SRB vor dem Europäischen Gericht (EuG).[10] Nachdem das EuG zugunsten des SRB urteilte, wandte sich der EDSB in der nächsten Instanz an den EuGH.

Für Stellen der EU gilt bei der Verarbeitung personenbezogener Daten gemäß Art. 2 Abs. 3 DSGVO nicht die DSGVO, sondern besondere Vorschriften. Diese sind seit 2018 in einer separaten Datenschutzverordnung (DSVO)[11] festgelegt. Für den SRB als EU-Behörde gilt entsprechend die DSVO, sodass das Urteil die datenschutzrechtlichen Fragen anhand dieser DSVO behandelt.

---

5 Vgl. EuGH, Urt. v. 19.10.2016, Rs. C-582/14 – Breyer, Rn. 41-46.

6 Zu den genauen technischen Möglichkeiten siehe IT-Planungsrat, Becker, Handreichung Anonymisierung, 28.4.2024, S. 27-40, https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/schwerpunktthemen/2025_04_22_Handreichung_Anonymisierung_final.pdf (Alle Links dieses Beitrags wurden zuletzt am 15.12.2025 abgerufen).

7 Ernst, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, DSGVO Art. 4 Rn. 50.

8 So zum Beispiel in diesem Bericht über eine Studie aus dem Jahr 2019: https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten/.

9 Zum Sachverhalt siehe EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 9-28.

10 Dazu ausführlich Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.

11 Verordnung (EU) 2018/1725.

Der Begriff der „personenbezogenen Daten“ ist jedoch im europäischen Datenschutzrecht identisch auszulegen,[12] sodass im Folgenden die Vorschriften der für Hochschulen und Forschungseinrichtungen relevanten DSGVO verwendet werden.

1. Personenbezogene Daten – was bedeutet Identifizierbarkeit?

Im Urteil werden zentrale Fragen des europäischen Datenschutzrechts behandelt. Im Mittelpunkt steht der Begriff der „personenbezogenen Daten“. Nach Art. 4 Nr. 1 DSGVO sind dies „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Der EuGH entschied zu mehreren Bestandteilen dieser Definition. Zunächst ging es um die Frage, ob die Stellungnahmen als „Informationen“ i.S.d. Art. 4 Nr. 1 DSGVO zu klassifizieren seien. Der EuGH bestätigte eine weite Auslegung von „Informationen“ und verwies auf seine frühere Rechtsprechung. Stellungnahmen, die Informationen „über“ eine Person und persönliche Meinungen oder Sichtweisen enthalten, sind personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO.[13]

Folgenreicher sind jedoch die grundlegenden Aussagen des EuGH zur „Identifizierbarkeit“ einer natürlichen Person. Insbesondere lehnte der Gerichtshof ein absolutes Verständnis[14] des Personenbezugs deutlich ab. Für die Identifizierbarkeit ist es nicht ausreichend, wenn die Daten von „irgendeiner Stelle“ zugeordnet werden können. Vielmehr bedarf es immer einer Einzelfallprüfung, ob die betroffene Person identifiziert oder identifizierbar ist oder die Daten anonym sind.[15] So stellte der EuGH fest, dass pseudonymisierte Daten „[…] nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden [müssen]. Denn die Pseudonymisierung kann – je nach Umständen des Einzelfalls – andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, [sodass] letztere für sie nicht oder nicht mehr identifizierbar ist.“[16] Der Begriff der „personenbezogenen Daten“ ist zwar weit zu verstehen, aber gerade nicht unbegrenzt.[17]

Der EuGH begründet diese Entscheidung wie folgt: Erstens ist die Pseudonymisierung kein Element der Definition von „personenbezogene[n] Daten“ in Art. 4 Nr. 1 DSGVO, sondern nur eine technische und organisatorische Umsetzung von Maßnahmen, die das Risiko einer Identifizierung vermindern sollen.[18] Wenn geeignete Maßnahmen getroffen werden, um eine Identifizierung zu verhindern, kann dies auch Auswirkungen auf den Personenbezug der Daten haben.[19] Zweitens zeigt eine Auslegung des ErwGr 26 Satz 3 und Satz 4, dass „alle Mittel“ und „alle objektiven Faktoren“, „die nach allgemeinem Ermessen wahrscheinlich genutzt werden“, bei der Beurteilung der Identifizierbarkeit berücksichtigt werden sollen.[20] Somit begründet das bloße Vorliegen von zusätzlichen Informationen noch nicht, dass personenbezogene Daten vorliegen, stattdessen bedarf es einer genaueren Prüfung.[21] Drittens bestätigte der EuGH seine Rechtsprechung, wonach sich der Personenbezug von Daten ändern kann.[22] So können an sich nicht personenbezogene Daten (zum Beispiel IP-Adressen) doch personenbezogen sein, wenn die rechtliche Möglichkeit besteht, die zusätzlichen Informationen

12 So auch der EuGH im Urteil, EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 52.

13 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 54, 60. Der EuG hatte noch eine eingehende Prüfung von Inhalt, Zweck und Auswirkungen der Stellungnahmen vorgesehen: EuG, Urt. v. 26.4.2023, Rs. T-557/20, Rn. 73 f.

14 Zu diesem relativen bzw. absoluten Verständnis siehe auch bereits Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.

15 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 69, 86.

16 Ibid., Rn. 86.

17 Ibid., Rn. 88.

18 Ibid., Rn. 72.

19 Ibid., Rn. 75.

20 Ibid., Rn. 79 f.

21 Ibid., Rn. 82.

22 Ibid., Rn. 83 f. mit Verweis auf die Rs. Breyer, Urt. v. 19.10.2016, Rs. C-582/14 und Rs. Gesamtverband Autoteile-Handel, Urt. v. 9.11.2023, Rs. C-319/22. Zu diesen Entscheidungen auch bereits Tech: Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.

zur Re-Identifizierung zu erhalten[23] oder auch, sofern die Daten anderen Personen überlassen werden, die über Mittel zur Re-Identifizierung verfügen.[24] Die Re-Identifizierungsmöglichkeiten sind somit auf eine konkrete Stelle bezogen. Sobald nicht ausgeschlossen werden kann, dass ein Datenempfänger die Daten doch zuordnen kann, liegen sowohl bei der Übermittlung als auch bezüglich einer späteren Verarbeitung personenbezogene Daten vor und die DSGVO ist weiterhin anwendbar (sogenannter indirekter Personenbezug).[25]

Im vorliegenden Fall konnte der SRB die Stellungnahmen und die zusätzlichen Informationen den jeweiligen Betroffenen jederzeit zuordnen. Die Daten wurden zwar pseudonymisiert, waren aber für den SRB weiterhin personenbezogene Daten.[26] Für den Datenempfänger, Deloitte, könnten die pseudonymisierten Stellungnahmen anonym sein, sofern Deloitte die Maßnahmen zur Pseudonymisierung nicht aufheben kann und eine Zuordnung in keinem Fall möglich ist.[27]

2. Gilt die Informationspflicht nach Art. 13 DSGVO, wenn die Daten für den Empfänger anonym sind?

Zusätzlich entschied der EuGH auch darüber, wie mit den Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person nach Art. 13 DSGVO umzugehen ist, wenn die pseudonymisierten Daten für den Datenempfänger anonym sind. Art. 13 Abs. 1 DSGVO legt als zeitliches Element der Informationspflicht den „Zeitpunkt der Erhebung dieser Daten“ fest. Der EuGH verwies entsprechend dem Wortlaut somit zunächst auf seine Rechtsprechung, wonach die Betroffenen sofort (bei Datenerhebung) zu informieren sind.[28] Die Identifizierbarkeit ist dabei aus Sicht des Verantwortlichen zu bestimmen.[29] Folglich spielt es für die Informationspflicht nach Art. 13 DSGVO keine Rolle, ob der Empfänger die Daten zuordnen kann oder ob sie für ihn anonym wären.[30] Der EuGH argumentiert dabei mit dem Sinn der Informationspflicht nach Art. 13 DSGVO. Danach sollen betroffene Personen durch die Informationen die Möglichkeit haben, mit voller Kenntnis der Sachlage über ihre personenbezogenen Daten bei der Datenerhebung zu entscheiden.[31] Zur vollen Sachlage gehören auch die potenziellen Empfänger. Somit müssen selbst Empfänger, für die die Daten anonym wären, vom Verantwortlichen genannt werden. Vorliegend entschied der EuGH, dass der SRB die betroffenen Personen über Deloitte als möglichen Empfänger der personenbezogenen Daten hätte informieren müssen.

III. Folgen des SRB-Urteils

Das SRB-Urteil hat in Fachkreisen zu vielen Diskussionen geführt. Insbesondere stellen sich nach diesem Urteil datenschutzrechtliche Folgefragen. Dies betrifft vor allem Situationen, in denen Daten ausgetauscht werden oder mehr als eine Stelle Daten verarbeitet und die Identifizierbarkeit der Daten auseinanderfällt.

1. Gemeinsame Verantwortung, Art. 26 DSGVO

Als Erstes stellt sich bereits die Frage, wie Konstellationen von zwei oder mehr Verantwortlichen[32] zu behandeln sind, wenn dieselben Daten von einem Verantwortlichen mithilfe von zusätzlichen Informationen zugeordnet werden können, also

23 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 83.

24 Ibid., Rn. 84.

25 Ibid., Rn. 85.

26 Ibid., Rn. 76.

27 Ibid., Rn. 77.

28 Ibid., Rn. 102.

29 Ibid., Rn. 111.

30 Ibid., Rn. 112.

31 Ibid., Rn. 108.

32 Allgemein zur gemeinsamen Verantwortung siehe Geiselmann, Gemeinsam sind wir verantwortlich!, DFN-Infobrief Recht 1/2024 sowie zur EuGH-Rechtsprechung Tech, Die Heiligen Drei der gemeinsamen Verantwortlichkeit, DFN-Infobrief Recht 12/2025.

personenbezogen sind, und für einen anderen Verantwortlichen wiederum keine tatsächlichen oder rechtlichen Möglichkeiten einer Zuordnung bestehen. Wenn zwei Stellen gemeinsame Entscheidungen über Zwecke und Mittel einer Verarbeitung treffen, spricht dies in der Regel für eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DSGVO. Wenn die Daten für eine der Stellen jedoch anonym sind, ist fraglich, ob die DSGVO für diese Stelle überhaupt Anwendung findet. Gerade dann sind jedoch umfangreiche Vorkehrungen zu treffen, um im Zweifel beweisen zu können, dass die Daten für die Stelle tatsächlich und dauerhaft anonym sind und auch bleiben.

2. Auftragsverarbeitung, Art. 28 DSGVO

Außerdem ist fraglich, wie mit der Auftragsverarbeitung nach Art. 28 DSGVO künftig umzugehen ist, wenn (wie in der Konstellation bei SRB und Deloitte) der Verantwortliche die Daten pseudonymisiert an einen Dienstleister übermittelt, für den die Daten anonym sind. Liegt dann noch eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO vor und bedarf es einer Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO? Immerhin definiert Art. 4 Nr. 8 DSGVO den Auftragsverarbeiter als eine Person, die „personenbezogene Daten im Auftrag des Verantwortlichen" verarbeitet. Dabei sind verschiedene Konstellationen und Szenarien zu unterscheiden, die jeweils genau durchgeprüft werden müssen. In diesem Zusammenhang könnte sich der Verantwortliche zumindest insofern zusätzlich absichern, indem er vertraglich mit dem Dienstleister vereinbart, dass eine Re-Identifizierung verboten ist.[33]

3. Datenübermittlungen, Art. 44 ff. DSGVO

Zuletzt verbleibt nach dem SRB-Urteil des EuGH die Frage, ob eine Rechtsgrundlage für die Weitergabe der Daten oder gerade auch im Kontext von Drittlandtransfers nach Art. 44 ff. DSGVO erforderlich ist und wessen Perspektive dafür heranzuziehen ist. Auch hier gilt es, die Situationen genaustens zu prüfen und Nachweise zu sammeln.

4. Digitaler Omnibus-Verordnungsentwurf

Mitte November 2025 veröffentlichte die EU-Kommission den Verordnungsentwurf zu einem digitalen Omnibus zur Änderung von Datengesetzen.[34] Dieser enthält – gerade im Datenschutzrecht – einige Anpassungen.[35] So will der Gesetzgeber die Rechtsprechung des EuGH gesetzlich verankern, indem er die Definition der „personenbezogenen Daten" in der DSGVO anpasst. Die Datenschutzkonferenz (DSK) sah die vorgeschlagenen Änderungen der DSGVO jedoch kritisch und will sich gerade bezüglich der Definition von „personenbezogenen Daten" noch ausführlich äußern.[36]

IV. Bedeutung für Hochschulen und Forschungseinrichtungen

Das SRB-Urteil ist auch für Hochschulen und Forschungseinrichtungen interessant. Zum einen betont das Urteil, dass datenschutzrechtliche Informationspflichten einzuhalten sind. Dies sollten auch Hochschulen und Forschungseinrichtungen als Verantwortliche nicht vernachlässigen. Zum anderen gilt auch für Hochschulen und Forschungseinrichtungen als Verantwortliche, dass künftig eine noch sorgfältigere Prüfung bei einer Weitergabe von pseudonymisierten Daten erfolgen muss. Das Urteil kann jedoch auch eine Chance für die Forschung sein. Bestimmte Forschungsprojekte und gerade das Training von KI-Modellen sind einfacher durchzuführen, wenn anonyme Daten verwendet werden. Sofern also beispielsweise personenbezogene Daten bei einer anderen Stelle verarbeitet und so pseudonymisiert an Hochschulen und Forschungseinrichtungen übermittelt werden, sodass diese keine Möglichkeit einer Re-Identifizierung haben, wären die Daten für die Hochschule oder Forschungseinrichtung anonym. Die tatsächlichen Folgen des SRB-Urteils könnten somit in vielerlei Hinsicht weitreichend sein.

---

33 So z. B. auch Nebel, CR 2025, 711, 716 Rn. 37.

34 COM (2025) 837 final, 19.11.2025, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

35 Zu den Reformvorschlägen der DSGVO ausführlich in dieser Infobrief-Ausgabe: Müller-Westphal, Alles bleibt anders, DFN-Infobrief Recht 2/2026.

36 Pressemitteilung vom 12.12.2025, S. 1 f., https://datenschutzkonferenz-online.de/media/pm/DSK_PM_110_DSK.pdf.

DFN Infobrief-Recht-Aktuell

• Telekommunikationsrecht: Entwurf der Europäischen Kommission vom 21. Januar 2026 zum Digital Network Act (DNA), der die EU-Vorschriften über Konnektivitätsnetze modernisieren, vereinfachen und harmonisieren soll

Mit dem DNA sollen die Voraussetzungen dafür geschaffen werden, dass Netzbetreiber in den Ausbau fortgeschrittener Glasfaser- und Mobilfunknetze investieren können. Ziel ist es, die Abschaltung der Kupfernetze und den Transfer zu fortschrittlichen Netzen im Zeitraum zwischen 2030 und 2035 zu gewährleisten. Unternehmen soll dadurch die Erbringung von Dienstleistungen in der gesamten EU erleichtert werden, indem sie sich nur noch in einem Mitgliedstaat registrieren lassen müssen. Zudem sollen Anreize für den Aufbau europaweiter Satellitenkommunikationsdienste geschaffen werden, indem ein Frequenzgenehmigungsrahmen auf EU-Ebene anstelle der nationalen Ebene eingeführt wird.

Hier erhalten Sie den Link zur Presseerklärung der Europäischen Kommission:
https://ec.europa.eu/commission/presscorner/detail/de/ip_26_107

• Plattformrecht: Entscheidung des Kammergerichts zur Löschung von Facebook-Gruppen

Das Kammergericht entschied am 23. Dezember 2025, dass kein Anspruch auf Löschung zweier kritischer Facebook-Gruppen besteht, wenn die Mehrzahl der Beiträge im sozialen Netzwerk rechtstreu ist und die Gruppe selbst nicht ausschließlich zur Rechtsverletzung eingerichtet wurde. Die Löschung der gesamten Gruppe sei unverhältnismäßig, auch wenn es durch Gruppenmitglieder wiederholt zu öffentlichen Beleidigungen sowie zu Mord- und Gewaltandrohungen gegen den Kläger gekommen sei.

Hier erhalten Sie den Link zur Presseerklärung des Kammergerichts:
https://www.berlin.de/gerichte/presse/pressemitteilungen-der-ordentlichen-gerichtsbarkeit/2025/pressemitteilung.1628932.php

• Cybersicherheitsrecht: Neues Cybersicherheitspaket der Europäischen Kommission

Da sich Europa täglich Cyberangriffen und hybriden Angriffen auf grundlegende Dienste und demokratische Institutionen ausgesetzt sieht, wurde am 20. Januar 2026 von der Europäischen Kommission ein neues Cybersicherheitspaket vorgeschlagen, um angesichts der zunehmenden Bedrohung die Widerstandsfähigkeit und die Fähigkeiten der EU im Bereich der Cybersicherheit zu stärken.

Hier erhalten Sie den Link zur Presserklärung der Europäischen Kommission:
https://ec.europa.eu/commission/presscorner/api/files/attachment/882208/Factsheet%20New%20Cybersecurity%20Package.pdf

• Datenrecht: Gesetzesentwurf zum Data Governance Act (DGA)

Der europäische Gesetzgeber hat durch den DGA Regelungen geschaffen, die die Weiterverwendung von Daten festlegen, die sich im Besitz öffentlicher Stellen befinden. Die Bundesregierung hat am 13. Januar 2026 einen Entwurf für ein Daten-Governance-Gesetz veröffentlicht, das der Umsetzung des DGA in nationales Recht dienen soll. Nationale Regelungen sind erforderlich, um Zuständigkeiten festzulegen und Sanktionen vorsehen zu können. Durch das Gesetz soll die Weiterverwendung geschützter Daten der öffentlichen Hand für Datenvermittlungsdienste und datenaltruistische Organisationen geregelt werden.

Hier erhalten Sie den Link zum Gesetzentwurf: https://dserver.bundestag.de/btd/21/035/2103544.pdf

Kurzbeitrag: Kehrtwende in der Plattformhaftung

Der Europäische Gerichtshof stellt mit einem Grundsatzurteil neue Weichen in der Plattformhaftung

von Anna Maria Yang-Jacobi, Berlin

Online-Plattformen sind für Inhalte Dritter auf ihren Diensten bis zur Kenntniserlangung grundsätzlich nicht verantwortlich. Ob dies auch für die datenschutzrechtliche Haftung gilt, fragte ein rumänisches Gericht den Europäischen Gerichtshof (EuGH). In seiner Entscheidung Russmedia räumte dieser nun der datenschutzrechtlichen Haftung den Vorrang ein. Die Entscheidung verschärft nicht nur die datenschutzrechtliche Haftung von Hostingdiensteanbietern. Sie könnte zu unvorhersehbaren Veränderungen des plattformbasierten Internets führen.

I. Ausgangspunkt: Haftungsprivileg für Vermittlungsdienste

Die Haftung digitaler Dienste für Inhalte, die von ihren Nutzenden hochgeladen werden, ist eine der Urfragen des Internets.[1] Das heutige Internet besteht im Wesentlichen aus einer Vielzahl digitaler Dienste. Die für den alltäglichen Gebrauch wichtigste Art von Diensten ist jene, die Speicherplatz für Informationen ihrer Nutzenden zur Verfügung stellt (Hostingdienste). Viele dieser Hostingdienste ermöglichen es ihren Nutzenden außerdem, die auf ihren Diensten gespeicherten Informationen öffentlich zu verbreiten (Online-Plattformen).[2] Dabei handelt es sich etwa um Online-Marktplätze, Foren, Video-Sharing-Dienste oder auch soziale Netzwerke.

Bereits in der Frühphase des Internets um die Jahrtausendwende wurde offensichtlich, dass den Betreibern derartiger Dienste erhebliche Haftungsrisiken drohen. Wer Millionen von Nutzenden die Möglichkeit bietet, Inhalte zur Verfügung zu stellen und zu teilen, kann kaum kontrollieren, wie diese Öffentlichkeit genutzt wird. Dadurch besteht die Gefahr, dass Diensteanbieter ungewollt die Infrastruktur für massenhafte Rechtsverletzungen bereitstellen und für die Beseitigung der dadurch entstehenden Schäden ohne Weiteres zur Verantwortung gezogen werden können. Gegebenenfalls könnten sie sogar strafrechtlich wegen Beihilfe zu Straftaten belangt werden.

Auf diese Risiken reagierte der Gesetzgeber, der das entstehende Internet als (ökonomische) Chance und Innovationsraum begriff. Nach US-amerikanischem Vorbild etablierte die Europäische Union in Art. 12-14 der E-Commerce-Richtlinie (EC-RL)[3] Haftungsprivilegierungen für Anbieter von Vermittlungsdiensten. Diese Haftungsprivilegierungen finden sich mittlerweile in Art. 4-6 des Digital Services Act (DSA). Sie besagen grob, dass Anbieter von Vermittlungsdiensten für fremde, rechtsverletzende Inhalte auf ihren Plattformen nicht verantwortlich sind, solange sie keine Kenntnis von der Rechtswidrigkeit des Inhalts haben. Sie haften also weder zivilrechtlich auf Schadensersatz, Beseitigung oder Unterlassung noch sind sie strafrechtlich verantwortlich.

---

1 Vgl. dazu Koseff, The Twenty-Six Words That Created the Internet (2019).

2 Art. 3 lit. g sublit. iii, lit. k, lit. i DSA. Ausführlich zu den verschiedenen Kategorien von Diensten von Bernuth, Die falbelhafte Welt der digitalen Dienste, DFN-Infobrief Recht 07/2025, 6-10.

3 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 („Richtlinie über den elektronischen Geschäftsverkehr“).

Die Haftungsprivilegien dienen somit zum einen der Innovationsförderung.[4] Zum anderen haben sie auch eine Dimension für die Ermöglichung gesellschaftlichen Austauschs. Die Privilegierungen begünstigen, dass die Anbieter Dienste auf den Markt bringen, mithilfe derer Nutzende frei und ohne vorherige Kontrolle Inhalte teilen und miteinander interagieren können.[5] Diese Haftungsprivilegierungen haben das Internet, wie wir es heute kennen, maßgeblich geprägt.

II. Die Russmedia-Entscheidung

Dieser Kontext ist entscheidend für das Verständnis und die Tragweite der Russmedia-Entscheidung des EuGH. Was war passiert? Eine unbekannte Person lud auf einer Online-Plattform des Russmedia-Konzerns eine Anzeige hoch, in der eine dritte Person, die spätere Klägerin, vermeintlich sexuelle Dienstleistungen anbot, einschließlich Fotos und Telefonnummer. Die Klägerin beschwerte sich bei Russmedia über die Anzeige und der Plattformanbieter entfernte sie umgehend. Doch bis dahin hatte sich die Anzeige bereits über den Kontrollbereich des Plattformanbieters hinaus im Internet verbreitet.

Daher verlangte die Klägerin von Russmedia immateriellen Schadensersatz für den Datenschutzverstoß nach Art. 82 Datenschutz-Grundverordnung (DSGVO). Der Fall nahm zunächst in Rumänien seinen Lauf und landete schließlich wegen offener unionsrechtlicher Fragen vor dem EuGH. Im Ergebnis sprach der EuGH der Klägerin den Schadensersatz zu. Der Fall wirft insbesondere zwei Problemkomplexe auf: Zum einen war fraglich, ob Russmedia als datenschutzrechtlich Verantwortlicher in Betracht kommt. Zum anderen stellte sich die Frage, ob Russmedia sich als Online-Plattform nicht auf das Haftungsprivileg in Art. 14 EC-RL (nun: Art. 6 DSA) berufen könnte.

1. Verantwortlichkeit

Unstreitig handelte es sich im vorliegenden Fall um einen Datenschutzverstoß. Der Schadensersatz nach Art. 82 DSGVO setzt aber auch voraus, dass der Anspruchsgegner Verantwortlicher oder Auftragsverarbeiter im datenschutzrechtlichen Sinne ist. Als Auftragsverarbeiter kann man sich zudem einfacher von der Haftung befreien. Nach Art. 4 Nr. 7 DSGVO ist Verantwortlicher, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Klar ist, dass die unbekannte Person, die die gefälschte Anzeige veröffentlichte, verantwortlich ist. Ob darüber hinaus aber auch Russmedia als Plattformanbieter verantwortlich ist, war jedoch fraglich.

Aus Sicht des EuGH ist Russmedia Verantwortlicher, da sich das Geschäftsmodell nicht im reinen Plattformangebot erschöpft. Die Inhalte der Nutzenden würden durch Russmedia auch zu eigenen, kommerziellen Zwecken verarbeitet, etwa zur Generierung von Werbeeinnahmen. Außerdem wirkt die Plattform durch ihre algorithmische Kuratierung auf die Mittel der Datenverarbeitung ein. Damit ist der Plattformanbieter nicht bloß Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO), sondern gemeinsam mit dem unbekannten Nutzer Verantwortlicher.
Diese Entscheidung überrascht nicht weiter und liegt im Einklang mit dem weiten Verständnis der datenschutzrechtlichen Verantwortlichkeit.

2. Haftungsprivileg

Um der datenschutzrechtlichen Haftung auf Schadensersatz zu entgehen, konnte Russmedia also nur noch auf das Haftungsprivileg hoffen. Das eingangs eingeführte Haftungsprivileg für Hostingdiensteanbieter findet sich in Art. 6 DSA. Demnach könnte Russmedia also erst dann für die Inhalte auf der eigenen Plattform haften, wenn sie von ihnen Kenntnis erlangt hat. Da Russmedia nach Meldung des Inhalts umgehend tätig wurde, könnte der Plattformanbieter im vorliegenden Fall vom Haftungsprivileg profitieren.

Doch die rumänischen Gerichte legten dem EuGH die Frage vor, ob das Haftungsprivileg im vorliegenden Fall der datenschutzrechtlichen Haftung überhaupt greifen könne. Es ging also im Kern um das Verhältnis der Haftungsprivilegierungen aus EC-RL (nun DSA) auf der einen und der Haftung nach der DSGVO auf der anderen Seite.

---

4 Erwägungsgründe 2, 40 EC-RL.

5 Hierzu auch Tuchtfeld, Verfassungsblog, 05.12.2025, https://verfassungsblog.de/eugh-russmedia-digital-uberwachung/ (alle Links dieses Beitrags zuletzt abgerufen am 10.12.2025).

Die Rechtsakte selbst bestimmen zu ihrem jeweiligen Verhältnis, dass sie sich „unberührt“ lassen. Diese gegenseitigen Klauseln sagen im Ergebnis aber nichts über den Vorrang der einen oder anderen Regelung. Der EuGH bewertet diese Rechtslage in der Entscheidung Russmedia vornehmlich aus der Perspektive des Datenschutzrechts. Nach Ansicht des Gerichts dürften die Haftungsprivilegierungen „auf keinen Fall“ die Anforderungen des Datenschutzrechts beeinträchtigen. Daher nimmt der Gerichtshof an, dass die datenschutzrechtliche Haftung unberührt bleiben muss und Russmedia nicht privilegiert ist.

III. Auswirkungen der Entscheidung

Die Entscheidung ist ein echter Paukenschlag für die Plattformhaftung – und damit für eine der Grundstrukturen des Internets. Der Fall betrifft zwar nicht die Haftungsprivilegien insgesamt, sondern alleine ihre Anwendbarkeit im Bereich des Datenschutzes. Doch in Streitigkeiten über Inhalte auf Plattformen sind nahezu immer personenbezogene Daten involviert – jeder dieser Fälle hat damit eine datenschutzrechtliche Dimension. Faktisch hat die Russmedia-Entscheidung daher zur Konsequenz, dass Plattformen in Zukunft nicht erst ab Kenntnis, sondern von Beginn an für eine Vielzahl fremder Inhalte auf ihren Plattformen haften. Während einige Datenschutzbehörden die Entscheidung begrüßen, geht die Literatur kritisch mit ihr ins Gericht. Eine mögliche Folge dieser Haftungsrisiken könnte der flächendeckende Einsatz algorithmischer Filtersysteme sein, die jeden hochzuladenden Inhalt auf etwaige Datenschutzverstöße prüfen. Im Zweifel veröffentlicht die Plattform legale Inhalte im Grenzbereich dann lieber nicht (sog. Overblocking).

Es scheint, als habe der EuGH in der Entscheidung die grundlegende Systematik der Plattformhaftung nicht ausreichend in den Blick genommen. Die Haftungsprivilegien für Hostingdiensteanbieter galten bislang grundsätzlich umfassend und können nur so ihren eingangs beschriebenen Zweck erfüllen.

Die Entscheidung bewirkt eine echte Verschiebung im Bereich der Plattformhaftung. Dies kann auch für Hochschulen und Forschungseinrichtungen Auswirkungen haben, soweit diese etwa Lernplattformen oder ähnliche Dienste betreiben. Insbesondere sobald personenbezogene Daten involviert sind, droht Plattformanbietern nun bei Verstößen gegen die DSGVO eine unmittelbare Haftung auch für Inhalte Dritter. Eine Einschränkung der Haftung könnte über die Frage der Verantwortlichkeit erfolgen – hier stellte der EuGH in seiner Russmedia-Entscheidung im Wesentlichen auf die kommerzielle Ausrichtung des Plattformanbieters ab. Doch auch als Auftragsverarbeiter kommt eine Haftung nach Art. 82 DSGVO in Betracht.

Offen ist, ob die Entscheidung den europäischen Gesetzgeber auf den Plan rufen wird, um das Verhältnis zwischen Datenschutzhaftung und Privilegierungen im DSA zu konkretisieren. Es ist schwer vorstellbar, dass das Auslegungsergebnis des EuGH dem entspricht, was der europäische Gesetzgeber beim Fortschreiben der Haftungsprivilegierungen im DSA geplant hatte.

Impressum

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster und der Humboldt-Universität Berlin.

Humboldt-Universität zu Berlin
Lehrstuhl für Bürgerliches Recht und Recht der Digitalisierung

Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Unter den Linden 11, 10117 Berlin

Tel. (030) 838-66754

E-Mail: recht@dfn.de

Universität Münster
Institut für Informations-, Telekommunikations- und Medienrecht
-Zivilrechtliche Abteilung-

Leonardo Campus 9, 48149 Münster

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn