Verbraucherzentrale
Bundesverband

Digitaler Omnibus: Verfehlte Ziele, geschwächte Rechte

Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zu den Vorschlägen der Europäischen Kommission zur Vereinfachung des digitalen Rechtsrahmens („Digital Omnibus“) (2025/0360(COD)).

12. Dezember 2025

Inhalt

I. Verbraucherrelevanz

Digitale Dienste durchdringen den Alltag der Verbraucher:innen und prägen zentrale Lebensbereiche wie Kommunikation, Konsum und Informationszugang. Entscheidungen von Verbraucher:innen über die Nutzung solcher Dienste werden unter erheblichen Informationsasymmetrien getroffen: 70 Prozent der Verbraucher:innen äußerten sich im Consumer Conditions Scoreboard 2023 der Europäischen Kommission besorgt darüber, wie ihre personenbezogenen Daten verwendet und weitergegeben werden. 38 Prozent berichteten in diesem Zusammenhang von einem Rückgang ihres Vertrauens in den elektronischen Handel.[1] Auch andere Studien belegen, dass Datenschutzbedenken zu den Hauptgründen zählen, wenn Verbraucher:innen bestimmte digitale Angebote meiden.[2]

Demgegenüber bedeutet ein hohes Datenschutzniveau Vereinfachung und Entbürokratisierung für Verbraucher:innen. So unterstreichen empirische Daten, dass deren Vertrauen eine essenzielle Voraussetzung für die Nutzung digitaler Dienste und für eine starke Markenbindung ist: In einer aktuellen Umfrage des Verbraucherzentrale Bundesverbands (vzbv)[3] gaben 63 Prozent der befragten Verbraucher:innen an, Unternehmen die der Datenschutz-Grundverordnung (DSGVO) unterliegen, im Umgang mit ihren Daten deutlich oder etwas mehr zu vertrauen. Zugleich ist es 87 Prozent der Befragten sehr oder eher wichtig, dass sie Unternehmen im Umgang mit ihren persönlichen Daten vertrauen können, bevor sie deren Angebote nutzen.

Hohe Datenschutzstandards können damit unmittelbar die Bereitschaft beeinflussen, bestimmte digitale Dienste in Anspruch zu nehmen und einen Standortvorteil für europäische Unternehmen schaffen, deren Angebote auf einem rechtlich gesicherten Schutzniveau beruhen. Ein kohärenter, verlässlicher Datenschutzrahmen bleibt damit eine Voraussetzung für funktionierende Märkte, starke Verbraucherrechte und eine nachhaltige digitale Ökonomie.

II. Zusammenfassung

Mit den vorliegenden Vorschlägen können die Ziele des Digitalen Omnibusses in weiten Teilen nicht erreicht werden. Hinsichtlich der Anpassung der DSGVO findet keine Vereinfachung des Rechts statt; stattdessen entstehen neue unbestimmte Begriffe, komplexe Ausnahmekataloge und zusätzliche Abwägungsanforderungen. Rechtssicherheit wird nicht gestärkt, sondern geschwächt, divergierende Auslegungen zwischen Mitgliedstaaten und Gerichten mit langwierigen Verfahren sind vorprogrammiert. Eine Entlastung kleiner und mittlerer Unternehmen ist nicht erkennbar, es

---

[1] European Commission: Consumer Conditions Scoreboard, 2023, S. 20, https://commission.europa.eu/system/files/2023-10/consumer_conditions_scoreboard_2023_v1.1.pdf, 01.10.2025.

[2] Bitkom: Mehr als jeder Dritte hat Hemmungen, digitale Angebote zu nutzen, 2025, https://www.bitkom.org/Presse/Presseinformation/Hemmungen-digitale-Angebote-Digitaltag-2025, 02.10.2025.

[3] Verbraucherzentrale Bundesverband: Jahresendbefragung. Tabellenband, 2025, S. 3f, https://www.vzbv.de/sites/default/files/2025-12/Tabellenbaender_vzbv_Datenschutz.pdf, 12.12.2025.

entstehen neue Risiken durch unklare Geltungsvoraussetzungen und zusätzliche Compliance-Unsicherheiten. Auch die Kohärenz des europäischen Digitalrechts wird nicht verbessert, vielmehr sind neue Konflikte zu erwarten. Schließlich wird auch der Grundrechtsrahmen nicht gestärkt, zentrale Grundprinzipien wie Transparenz, Zweckbindung und Rechenschaftspflicht werden unterlaufen. Eine Reform, die diese grundlegenden Ziele verfehlt, kann keinen Beitrag zu einem modernen, verhältnismäßigen und verlässlichen Digitalrechtsrahmen leisten.

Dadurch ergeben sich erhebliche Risiken für Verbraucher:innen und europäische Unternehmen. Gerade große, überwiegend außereuropäische Tech-Unternehmen profitieren, weil sie aufgrund ihrer globalen Dateninfrastruktur und umfangreichen Rechts- und Technikressourcen komplexe Ausnahmebestimmungen und offene Rechtsbegriffe leichter operationalisieren können, während kleinere europäische Anbieter mit Unsicherheiten und zusätzlichem Compliance-Aufwand konfrontiert werden.[4] Für Verbraucher:innen entstehen Risiken, weil datenintensive Verarbeitungen erleichtert werden und sie gleichzeitig über geringere Kontroll- und Durchsetzungsmöglichkeiten verfügen. Ein sinkendes Vertrauen in digitale Dienste wäre eine absehbare Folge.

Der vzbv fordert daher:

- Eine Reform des europäischen Digitalrechts muss auf klaren Problemdefinitionen, transparenter Konsultation, belastbarer Evidenz und einer vollständigen Folgenabschätzung gemäß der **Better-Regulation**-Vorgaben der Europäische Kommission beruhen.
- Die **Neudefinition personenbezogener Daten muss gestrichen werden**. Eine europarechtlich tragfähige Definition darf nur auf der EuGH-Rechtsprechung und dem bestehenden objektiven Identifizierbarkeitsmaßstab der DSGVO aufbauen und darf nicht darüber hinaus gehen.
- Die vorgeschlagene **Definition des Forschungsbegriffs muss verworfen werden**. Europarechtlich tragfähige Erleichterungen für gemeinwohlorientierte Forschung erfordern einen klar konturierten, methodisch-wissenschaftlichen Forschungsbegriff, der Zweckbindung, Transparenz und die Schutzmechanismen aus Art. 89 DSGVO nicht schwächt. Es bedarf präziser operationalisierter Garantien, nicht pauschaler Ausnahmen.
- Die **Einschränkung des Auskunftsrechts muss gestrichen werden**. Statt Rechtsklarheit zu schaffen, würde der Vorschlag gefestigte EuGH-Rechtsprechung infrage stellen, neue Auslegungsunsicherheiten erzeugen und voraussichtlich erneute Klärungsverfahren erfordern. Das Auskunftsrecht muss ohne Motivprüfung und ohne zusätzliche Voraussetzungen anwendbar bleiben.
- Die **Abschwächung der Informationspflichten muss gestrichen werden**. Transparenzpflichten müssen auf objektiven Kriterien beruhen und dürfen nicht durch Kontextvermutungen ersetzt werden. Eine Kenntnisfiktion ist mit dem Transparenzgrundsatz und mit Art. 8 Grundrechtecharta (GRCh) unvereinbar. Sinnvolle Vereinfachungen der Transparenzpflichten können außerhalb materieller Änderungen der DSGVO erfolgen: Einheitliche Kurztexte und Piktogramme für typische Verarbeitungsvorgänge könnten Unternehmen bei der Erfüllung ihrer Informationspflichten unterstützen und gleichzeitig die Verständlichkeit für Verbraucher:innen erhöhen.

[4] Vgl. Schaake, Marietje; Thun, Max von: Europe's Tech Sovereignty Demands More Than Competitiveness, 2025, https://www.project-syndicate.org/commentary/europe-misguided-fixation-on-enhanching-tech-competitiveness-by-marietje-schaake-and-max-von-thun-2025-04, 08.12.2025.

- Die **Überführung der „Cookie“-Regelungen in die DSGVO muss überarbeitet werden.** Der präventive Schutz aus Art. 5 (3) ePrivacy-Richtlinie sollte beibehalten werden. Mindestens aber brauchen die geplanten Ausnahmen klare Zweckgrenzen, technische Mindestanforderungen, ein ausdrückliches Weiterverarbeitungsverbot sowie – für die Reichweitenmessung – ein jederzeit ausübbares Widerspruchsrecht. Die Sicherheitsschranke muss präzise gefasst und auf notwendige Maßnahmen begrenzt werden. Dark Patterns müssen ausgeschlossen werden. Um Verbraucher:innen wirksam zu schützen und Unternehmen zu entlasten, wäre es jedoch insgesamt zielführender, Tracking und Profilbildung zu Werbezwecken zu untersagen.
- Die **Einführung automatisierter, maschinenlesbarer Präferenzsignale ist im Ansatz richtig** – die **Vorschläge werden aber auf unabsehbare Zeit nicht zu einer geringeren Anzahl an Einwilligungsbannern führen**. Die Pflicht der Verantwortlichen muss eindeutig und verbindlich ausgestaltet sein, die Ausnahme für Medienanbieter ist systemwidrig und sollte gestrichen werden. Notwendig ist zudem eine technische Spezifikation, die klare semantische Vorgaben, einfache Widerrufsmöglichkeiten, ein wirksames Verbot manipulativer Praktiken und die automatische Blockierung sämtlicher Tracking-Technologien bei aktivem Ablehnungssignal sicherstellt. Browser-, Betriebssystem- und App-Anbieter sowie andere Endnutzerumgebungen sind gleichermaßen einzubeziehen und so zu regulieren, dass ihre Gatekeeper-Position nicht zulasten der Verbraucher:innen wirkt.
- Die **Ausnahme vom Verarbeitungsverbot sensibler Daten für KI-Entwicklung und -Betrieb muss gestrichen werden**. Verantwortliche sollten auf die bestehenden, eng umrissenen Ausnahmetatbestände des Art. 9 (2)(a) bis (j) DSGVO verwiesen werden, die ein ausgewogenes und grundrechtlich tragfähiges Schutzniveau gewährleisten.
- Die Verarbeitung personenbezogener Daten für das **KI-Training erfordert eine eigenständige Rechtsgrundlage** mit strengen materiellen Voraussetzungen: Hierfür erforderlich ist ein Nachweis der Subsidiarität gegenüber synthetischen oder anonymisierten Daten, eine spezifische Risikoinformation vor Beginn der Verarbeitung, ein wirksames Widerspruchsrecht auch für Dritte ohne Nutzerkonto, klare technische Schutzmaßnahmen gegen Reproduktion und Identifizierbarkeit sowie ein Einwilligungserfordernis für Daten von Kindern.

III. Einleitung

Mit ihrem Vorschlag für eine Digital-Omnibus-Verordnung[5] vom November 2025 will die Europäische Kommission die Anwendung des europäischen digitalen Regelwerks optimieren.[6] Die geplanten Änderungen sollen Unternehmen und Bürger:innen entlasten und die Wettbewerbsfähigkeit stärken. Sie sollen die Einhaltung der Vorschriften kostengünstiger gestalten, die bisherigen Vorgaben wahren und verantwortungsbewussten Unternehmen einen Wettbewerbsvorteil verschaffen.

Eine Vereinfachung des europäischen Digitalrechts ist grundsätzlich sinnvoll.[7] Der bestehende Ordnungsrahmen ist über viele Rechtsakte verteilt, teilweise inkonsistent und für Verbraucher:innen wie Unternehmen schwer überschaubar. Selbst Expert:innen können die Wechselwirkungen der verschiedenen Rechtsakte kaum mehr überblicken. Eine Vereinfachung, Konsolidierung und bessere Abstimmung wären daher wünschenswert. Die nun vorgeschlagene Omnibus-Reform erfüllt diese Ziele jedoch nicht. Vielmehr verschiebt sie systematisch den Schutzbereich der DSGVO, etwa indem sie Definitionen und Rechtsgrundlagen ändert.

Besonders problematisch sind erhebliche Defizite im bisherigen Gesetzgebungsverfahren. Die Reformvorschläge wurden ohne belastbare Evidenz, ohne angemessene öffentliche Konsultation und ohne Folgenabschätzung vorgelegt. Etwaige DSGVO-Änderungen waren nicht Gegenstand des Call for Evidence vom September 2025[8], obwohl der Reformvorschlag acht Wochen vor seiner Veröffentlichung bereits existiert haben muss. Die paritätisch besetzte „GDPR Multistakeholder Expert Group“ der Europäischen Kommission wurde nicht einbezogen, obwohl sie genau für diese Fälle geschaffen wurde. Parallel durchgeführte „Reality Checks“ waren unausgewogen und durch wirtschaftliche Interessen geprägt.[9] Ein Verfahren, das substanzielle Grundrechtseingriffe vorsieht, darf aber nicht auf informellen Formaten mit unausgewogener Beteiligung aufgebaut werden. Dies widerspricht den eigenen Better-Regulation-Vorgaben[10] der Europäischen Kommission, die Konsultationen, Transparenz und eine belastbare Folgenabschätzung vorsehen. Die Vorschläge werden jedoch als „technische Anpassungen“ deklariert und damit aus dem ordentlichen Gesetzgebungsprozess herausgelöst, obwohl sie zentrale Strukturen der DSGVO neu definieren.

Der politische Kontext verschärft diese Kritik. Aus Sicht des vzbv ist es verfehlt, Datenschutz pauschal als Hemmnis für Wettbewerbsfähigkeit und technologische Innovation darzustellen. Es fehlen belastbare empirische Nachweise für innovationshemmende Effekte eines strengen

---

[5] Neben Änderungen an der DSGVO schlägt die Europäische Kommission im Rahmen des Digital Omnibus vor, das „data legislative acquis“ zu konsolidieren. Rechtsakte wie der „Data Governance Act“, die „Free Flow of Non-Personal Data Regulation“ und die „Open Data Directive“ sollen dabei in den „Data Act“ integriert und angepasst werden. Diese Vorschläge werden in der vorliegenden Stellungnahme nicht behandelt. Gleiches gilt für den parallel vorgeschlagenen „Digital Omnibus on AI (COM(2025) 836)“, zu dem der vzbv eine eigene Stellungnahme abgegeben hat.

[6] Vgl. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

[7] Siehe Verbraucherzentrale Bundesverband: DSGVO: Entlastung ja – Aufweichung nein, 2025, https://www.vzbv.de/sites/default/files/2025-05/25-05-07_Kurzstellungnahme_vzbv_DSGVO-Vereinfachung.pdf, 08.12.2025.

[8] Vgl. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus_en

[9] Corporate Europe Observatory: Preparing a roll-back of digital rights: Commission's secretive meetings with industry, 2025, https://corporateeurope.org/en/2025/11/preparing-roll-back-digital-rights-commissions-secretive-meetings-industry, 08.12.2025.

[10] Siehe European Commission: Better Regulation Guidelines, 2001, https://commission.europa.eu/document/download/d0bbd77f-bee5-4ee5-b5c4-6110c7605476_en?filename=swd2021_305_en.pdf, 08.12.2025.

Datenschutzes.[11] Im Gegenteil zeigen unter anderem die Evaluationsberichte der Europäischen Kommission aus den Jahren 2020 und 2024 sowie das dazu eingeholte Stakeholder-Feedback, dass kein struktureller Reformbedarf im Hinblick auf die DSGVO besteht. Die Europäische Kommission betonte vielmehr, dass die Grundsätze und Regelungen der DSGVO wirksam, zukunftsfähig und verhältnismäßig sind.[12] Ebenso wurde im Rahmen des von Michael McGrath, Europäischer Kommissar für Demokratie, Justiz, Rechtsstaatlichkeit und Verbraucherschutz, geleiteten GDPR Implementation Dialogs[13] im Juli 2025 deutlich, dass die DSGVO von Stakeholdern insgesamt als ausgewogener Rechtsrahmen wahrgenommen wird, der ihre Ziele erreicht hat. Unternehmen betonten zudem, dass sie bereits in Compliance investiert haben und eine Öffnung der DSGVO neue Unsicherheiten schaffen könnte.

Dennoch schlägt die Europäische Kommission weitreichende – und in weiten Teilen ungeeignete – Modifikationen der DSGVO vor. Diese Diskrepanz deutet darauf hin, dass politische Narrative stärker wirken als eine evidenzbasierte Problemanalyse. Geopolitischer Druck, zugunsten handelspolitischer Ziele Datenschutzstandards abzusenken, verschärft die Entwicklung.[14] Dieser Druck darf jedoch nicht zum Maßstab normativer Absenkungen werden. Die Verlässlichkeit des europäischen Rechtsrahmens und seine Grundrechtsorientierung gehören zu den zentralen Stärken der EU. Werden diese Prinzipien aufgegeben, verliert die EU ein wesentliches Alleinstellungsmerkmal.

IV. Allgemeine Anmerkungen

Inhaltlich fällt hinsichtlich der vorgeschlagenen DSGVO-Änderungen der selektive Umgang mit der Rechtsprechung des Europäischen Gerichtshofs (EuGH) sowie den Leitlinien des Europäischen Datenschutzausschusses (EDSA) auf. Einzelne Passagen aus Urteilen und Leitlinien werden überdehnt, um weitreichende strukturelle Änderungen zu rechtfertigen. Gleichzeitig werden klärende verbraucherschützende Interpretationen und Leitentscheidungen des EuGH – wie zur Reichweite von Auskunftsersuchen (C-154/21 *Österreichische Post AG*[15]) oder zur Tragweite des

[11] Siehe Bernd Beckert u. a.: Die Digitalisierung aus Innovationsperspektive. Faktencheck und Handlungsbedarf. Policy Brief 01/2021, S. 13, https://www.isi.fraunhofer.de/content/dam/isi/dokumente/policy-briefs/policy_brief_digitalisierung.pdf, 08.12.2025.

[12] European Commission: Second Report on the application of the General Data Protection Regulation. COM(2024) 357 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0357, 08.12.2025.

[13] Dass.: GDPR Implementation Dialogue: Summary Conclusions, 2025, https://commission.europa.eu/document/download/835dfd02-a38c-4cc3-ba53-5b0499e2b8b9_en?filename=Summary%20Conclusions%20Implementation%20Dialogue%20on%20the%20GDPR.pdf, 08.12.2025.

[14] Breton, Thierry: The world's digital empires are jostling for power – in Europe, we can't afford to be useful idiots, 2025, https://www.linkedin.com/pulse/worlds-digital-empires-jostling-power-europe-we-cant-afford-breton-juxbe/, 08.12.2025.

[15] EuGH, Urteil vom 12.01.2023 – C-154/21 *Österreichische Post AG* https://curia.europa.eu/juris/document/document.jsf?text=&docid=269146&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, 08.12.2025.

Begriffs „ausschließlich automatisiert“ (C-634/21 *SCHUFA*[16]) – nicht berücksichtigt. Dieser selektive Umgang mit höchstrichterlicher Rechtsprechung führt zu einer inkohärenten dogmatischen Grundlage und unterminiert Rechtssicherheit.

Darüber hinaus wurden Wechselwirkungen und Konflikte sowohl innerhalb der Vorschläge als auch in Bezug auf den bestehenden Rechtsrahmen erkennbar übersehen. Dies zeigt sich etwa daran, dass zwar die Regelung des Art. 5 (3) der ePrivacy-Richtlinie in die DSGVO verschoben werden soll, diese aber aufgrund der geplanten Neudefinition personenbezogener Daten faktisch ihren Anwendungsbereich verlieren würde. Ähnliches gilt für die vorgeschlagenen KI-Regelungen: Auch hier wird ein neuer Rechtsrahmen geschaffen, der aufgrund der geplanten Neudefinition personenbezogener Daten keinerlei Schutzwirkung entfalten könnte.

Insgesamt werden Auswirkungen der Vorschläge also erst in der Gesamtschau deutlich, da sich die Eingriffe gegenseitig verstärken und sich so der datenschutzrechtliche Schutzrahmen strukturell verschiebt. Ohne eine Analyse der kumulativen Effekte entsteht jedoch kein kohärentes Reformkonzept, sondern eine Sammlung isolierter Eingriffe, die in der Summe die Grundstruktur des Datenschutzrechts verändern. Die Better-Regulation-Vorgaben der Europäischen Kommission existieren gerade, um solche strukturellen Defizite zu vermeiden.

> Eine Vereinfachung der europäischen Digitalgesetzgebung muss auf klaren Problemdefinitionen, transparenter Konsultation, belastbarer Evidenz und einer vollständigen Folgenabschätzung beruhen. Die jetzige Reform erzeugt neue Unsicherheiten, verschiebt dogmatische Strukturen und schwächt bestehende Schutzmechanismen. Sie birgt erhebliche Risiken, leistet keinen Beitrag zu einem kohärenten und zukunftsfähigen Digitalrechtsrahmen und läuft der Stärkung des europäischen Binnenmarkts entgegen.

V. Positionen im Einzelnen

1. Kritische Änderungen zentraler Begriffsbestimmungen

1.1 Zur Neudefinition personenbezogener Daten

Ergänzung des Art. 4 (1) DSGVO / neuer Art. 41a DSGVO

Die Europäische Kommission schlägt vor, die Definition personenbezogener Daten so zu ändern, dass Informationen nur noch als personenbezogen gelten, wenn die jeweils verarbeitende Entität den Betroffenen identifizieren kann (Art. 3 (1)(a) des Digital Omnibus Entwurfs (folgend: DO-E)).

[16] EuGH, Urteil vom 07.12.2023 – C-634/21 *SCHUFA* https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, 08.12.2025.

Daten, die ein Empfänger nicht zuordnen kann, sollen für diesen nicht mehr als personenbezogen gelten, selbst wenn dritte Akteure identifizierungsfähig wären. Ergänzend soll die Europäische Kommission per Durchführungsrechtsakt festlegen können, wann pseudonymisierte Daten für bestimmte Empfänger nicht mehr personenbezogen sind (Art. 3 (10) DO-E).

Art. 4 (1) DSGVO-E ist keine bloße technische Klarstellung, sondern greift tief in die dogmatische Struktur der DSGVO und die einschlägige EuGH-Rechtsprechung ein. Das Urteil C-413/23 P *SRB*[17], das mit dem Vorschlag vermeintlich umgesetzt werden soll, wird selektiv interpretiert und deutlich überdehnt. Der EuGH hat in dem Urteil keine abstrakte Entitätslogik geschaffen, sondern eine Einzelfallprüfung bestätigt (Rn. 86, 100). Diese richtet sich nach Kosten, Zeit, technologischen Möglichkeiten und den Mitteln Dritter, die wahrscheinlich zur Identifikation eingesetzt werden können. Pseudonymisierte Daten sind demnach nur in eng begrenzten Ausnahmefällen für einen Empfänger nicht personenbezogen. Für Verantwortliche bleiben sie personenbezogen und werden bei Weitergabe an identifizierungsfähige Dritte – entgegen den Kommissionsvorschlägen – wieder zu personenbezogenen Daten (Rn. 81, 84, 85).

Die Änderung widerspricht der weiterhin geltenden Definition personenbezogener Daten und schwächt damit zentrale Rechte und Freiheiten Betroffener. So schließt die DSGVO auch Online-Kennungen und Fälle des „Singling-out“ ein, also der eindeutigen Wiedererkennbarkeit einer Person ohne Klardaten.[18] Das Konzept ist zentraler Bestandteil der bisherigen EuGH-Linie.[19] Die Aufgabe dieser Dimension würde Tracking-IDs, Hashwerte und segmentierende Kategorien privilegieren, die faktisch wie direkte Identifikatoren wirken. [20] Unternehmen könnten zudem durch organisatorische Trennungen oder das Auslagern von Schlüsselmaterial Konstruktionen schaffen, die formelle Nicht-Identifizierbarkeit behaupten, ohne faktische Re-Identifizierbarkeit zu verhindern.

Die Funktion der Pseudonymisierung wird systematisch verkannt. Sie stellt in erster Linie eine technische und organisatorische Schutzmaßnahme dar,[21] ist jedoch keine Anonymisierung. Eine „prohibition against reidentification“ ersetzt keinen technischen Schutz und verhindert nicht, dass Dritte – etwa in Datenhandelsketten, durch technologische Fortschritte oder außerhalb Europas – Betroffene re-identifizieren können. Der Vorschlag setzt zudem Fehlanreize: Unternehmen hätten weniger Anlass, in robuste Anonymisierungsverfahren zu investieren, wenn schwache Pseudonymisierung genügt, um die Anwendung der DSGVO auszuschalten.

Bedenklich ist auch, dass in Konstellationen, in denen pseudonymisierte Daten für einen Empfänger nicht mehr als personenbezogen gelten sollen, weder die Vorgaben zur Auftragsverarbeitung noch zur gemeinsamen Verantwortlichkeit zuverlässig greifen würden.

Insgesamt könnten Aufsichtsbehörden faktisch kaum noch überprüfen, ob Identifizierbarkeit ausgeschlossen ist. Die parallel geplante Absenkung der Anforderungen an Unternehmen bei Dokumentationspflichten (2025/0130/COD) würden diese Kontrolle weiter erschweren.

---

[17] EuGH, Urteil vom 04.09.2025 – C-413/23 P *SRB* https://curia.europa.eu/juris/document/document.jsf?text=&docid=303863&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=2488988, 08.12.2025.

[18] ErwGr. 26 DSGVO.

[19] Siehe etwa EuGH, Urteil vom 20.12.2017 – C-434/16 *Nowak*; EuGH, Urteil vom 07.03.2024 – C-604/22 *IAB Europe*

[20] Siehe auch Dachwitz, Ingo; Meineck, Sebastian: Databroker Files: Targeting the EU, 2025, https://netzpolitik.org/2025/databroker-files-targeting-the-eu/, 08.12.2025.

[21] Siehe auch Rn. 72 des EuGH-Urteils C-413/23 P *SRB*

Besonders kritisch ist die Kompetenzverschiebung durch den in Art. 41a DSGVO-E vorgesehenen Durchführungsrechtsakt, der die Definitionsmacht über den Schutzbereich eines Grundrechts auf die Exekutive verlagert. Die Frage, wann Daten nicht mehr personenbezogen sind, betrifft den Kern des Schutzbereichs von Art. 8 GRCh, der historisch auf der Systematik der Datenschutzrichtlinie 95/46 beruht – einschließlich der Definition personenbezogener Daten. Diese Verschiebung steht zudem im Spannungsverhältnis zu Art. 8 (3) GRCh, der es den unabhängigen Aufsichtsbehörden zuweist, die Anwendung des Datenschutzrechts zu kontrollieren.

Für Betroffene wären die Auswirkungen gravierend. Ob Daten personenbezogen sind, hinge künftig nicht mehr vom Inhalt ab, sondern davon, wer sie hält. Betroffene müssten für jeden Datenempfänger gesondert prüfen, ob die DSGVO gilt. Rechte auf Auskunft, Löschung, Zweckbindung und Rechenschaftspflicht ließen sich leicht abstreiten, wenn der Empfänger fehlende Identifizierbarkeit behauptet. Zudem entsteht ein zirkuläres Problem: Betroffene müssten zunächst Identifizierbarkeit nachweisen, um Auskunft nach Art. 15 DSGVO zu erhalten. Da diese Informationen jedoch typischerweise erst aus einem Auskunftsersuchen hervorgehen, entsteht ein faktisch unauflösbarer Widerspruch. Dies schwächt die praktische Durchsetzbarkeit der Betroffenenrechte und verschiebt das Schutzniveau zulasten der Verbraucher:innen.

Der Vorschlag erreicht damit das Gegenteil seines Ziels. Anstatt Klarheit zu schaffen, würde er jahrelange Rechtsunsicherheit erzeugen. Identifizierbarkeit wäre in unzähligen Einzelfällen (etwa auch beim KI-Training) strittig, die Reichweite der DSGVO für Betroffene wie Verantwortliche kaum noch bestimmbar. Das Fundament der DSGVO würde fragmentiert und verantwortungsbewusste Akteure gerieten gegenüber solchen in Nachteil, die gezielt organisatorische Blindstellen nutzen.

> Die vorgeschlagene Änderung ist nicht haltbar und muss vollständig gestrichen werden. Eine europarechtlich tragfähige Klarstellung kann nur auf dem bestehenden objektiven Identifizierbarkeitsmaßstab der DSGVO und der EuGH-Rechtsprechung aufbauen. Etwaige Anpassungen dürfen ausschließlich die methodische Präzisierung der Einzelfallprüfung betreffen – ohne Absenkung des Schutzbereichs oder Umdeutung der Pseudonymisierung.

1.2 Zur Definition des Forschungsbegriffs

Neuer Art. 4 (38) DSGVO / Neufassung des Art. 5 (1)(b) DSGVO / Ergänzung des Art. 13 (5) DSGVO

Der Entwurf weitet den Forschungsbegriff erheblich aus. Forschung soll künftig „any research which can also support innovation“ umfassen, einschließlich der Anwendung von „existing knowledge in novel ways“ zu „commercial interest“ (Art. 3 (1)(b) DO-E). Zusätzlich solle eine Weiterverarbeitung für Forschungszwecke stets als mit dem ursprünglichen Zweck vereinbar gelten (Art. 3 (2) DO-E). Informationen gegenüber Betroffenen können entfallen, wenn sie unmöglich, unverhältnismäßig oder forschungsgefährdend wären (Art. 3 (6) DO-E). Zudem wird Forschung in ErwGr. 32 DO-E zu einem berechtigten Interesse im Sinne des Art. 6 (1)(f) DSGVO erklärt.

Erleichterungen für gemeinwohlorientierte Forschung wären zwar grundsätzlich sinnvoll, die Vorschläge verschieben jedoch den Forschungsbegriff grundlegend. Forschung wird von einem methodisch-wissenschaftlichen Konzept zu einer weit gefassten Innovationskategorie, die nahezu jede datenintensive Tätigkeit einschließt. Die Definition verzichtet auf methodische Mindeststandards und verwendet unbestimmte Formulierungen wie „can support innovation“,

„aim of contributing to growth of society's knowledge and wellbeing" oder „apply existing knowledge in novel ways".[22] Damit eröffnet sie breite Missbrauchspotenziale, da Unternehmen Forschungserklärungen abgeben können, ohne dass ihnen wissenschaftliche Methodik, systematische Erkenntnisorientierung oder qualitätsgesicherte Verfahren zugrunde liegen.

Die in Art. 5 (1)(b) DSGVO-E vorgeschlagene automatische Zweckkompatibilität schwächt die Zweckbindung als zentralen Schutzmechanismus. Sie verliert ihre Funktion als materielle Schranke, wenn jede Weiterverarbeitung zu Forschungszwecken unabhängig von Art. 6 (4) DSGVO als legitim gilt. Verantwortliche könnten Daten für eng definierte Zwecke erheben und später für völlig andere Zwecke nutzen, solange sie dies unter den – künftig erweiterten – Forschungsbegriff subsumieren. Zugleich bleibt das Zusammenspiel mit den strengen Voraussetzungen für die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ungeklärt. Dies widerspricht der DSGVO-Systematik, der ständigen Rechtsprechung des EuGH sowie Art. 8 GRCh.

Die vorgesehenen Ausnahmen von Informationspflichten verschärfen diese Problematik. Kriterien wie „impossible", „disproportionate effort" oder „impair the achievement of the objectives" bergen das Risiko, nicht als Ausnahme, sondern als Regelinstrument zu wirken. Eine bloße öffentliche Bekanntmachung soll als Ersatz genügen, ohne dass Betroffene tatsächlich erreicht werden müssen. Dies schwächt Transparenzrechte erheblich, insbesondere bei sensiblen Daten.

Auch die vorgesehenen Schutzmaßnahmen bleiben insbesondere angesichts des uferlosen Forschungsbegriffs unzureichend. Verweise auf ethische Standards, Qualitätsanforderungen oder systematische Methoden bleiben inhaltsleer, da weder institutionelle Prüfmechanismen noch operationalisierte Kriterien vorgesehen sind. Zugleich verliert Pseudonymisierung ihre Schutzwirkung, weil nach der vorgeschlagenen Neudefinition personenbezogener Daten pseudonymisierte Daten für bestimmte Akteure als nicht personenbezogen gelten könnten.

ErwGr. 32 DO-E erweitert zudem den Anwendungsbereich von Art. 6 (1)(f) DSGVO, indem er Forschung pauschal als legitimes Interesse einordnet und damit die einzelfallbezogene Logik dieser Abwägungsnorm strukturell zugunsten datenintensiver Forschungs- und Innovationstätigkeiten verschiebt.

Insgesamt entsteht kein klarer, rechtsstaatlich belastbarer Rahmen für gemeinwohlorientierte Forschung, sondern ein entgrenzter Forschungsbegriff, der zentrale Schutzmechanismen der DSGVO – insbesondere Zweckbindung, Transparenz und Art. 89 DSGVO – erheblich schwächt. Betroffene können nicht mehr nachvollziehen, wann und mit welchen Zielen ihre Daten genutzt werden. Durch die so entstehende Rechtsunsicherheit geraten verantwortungsbewusste Akteure gegenüber solchen in Nachteil, die den weiten Forschungsbegriff strategisch nutzen.

> Die vorgeschlagenen Änderungen müssen verworfen werden. Europarechtlich tragfähige Erleichterungen für gemeinwohlorientierte Forschung erfordern einen klar konturierten, methodisch-wissenschaftlichen Forschungsbegriff, der Zweckbindung, Transparenz und die Schutzmechanismen aus Art. 89 DSGVO nicht schwächt. Es bedarf präziser operationalisierter

[22] So rechtfertigt etwa Meta bereits heute auf Grundlage des Artikel 6(1)(f) die Verarbeitung personenbezogener Daten (wie etwa „Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst") Betroffener - einschließlich Minderjähriger - auf Basis eines nahezu identischen Forschungsbegriffs: „Wir führen Umfragen durch und verwenden Informationen (u. a. von Forschern, mit denen wir zusammenarbeiten), um Forschung und Innovation zu Themen des sozialen Allgemeinwohls, des technologischen Fortschritts, des öffentlichen Interesses, der Gesundheit und des Wohlergehens durchzuführen und zu unterstützen." https://de-de.facebook.com/privacy/policy/; 08.12.2025.

> Garantien, nicht pauschaler Ausnahmen. Sinnvoll wäre ergänzend auch eine gezielte Stärkung institutioneller Strukturen, etwa eine engere Verzahnung von Datenschutzaufsicht und unabhängigen Ethikgremien sowie EU-weite Verhaltensregeln und Zertifizierungsmechanismen, die harmonisierte und überprüfbare Standards schaffen.[23]

2. Weitreichende Eingriffe in Betroffenenrechte und Transparenzpflichten

2.1 Zur Einschränkung des Auskunftsrechts

Neufassung des Art. 12 (5) DSGVO

Der Entwurf verändert das Auskunftsrecht grundlegend (Art. 3 (4) DO-E). Neben bestehenden Ablehnungsgründen soll eine neue Kategorie des „abuse of the right of access“ (durch Auskunftsersuchen „for purposes other than the protection of their data“) eingeführt werden, ergänzt durch einen abgesenkten Beweismaßstab („reasonable grounds to believe“). Zugleich sollen Betroffene Anfragen stärker präzisieren (ErwGr. 35 DO-E: „the data subject should be as specific as possible“). Breite oder undifferenzierte Anfragen könnten als „excessive“ zurückgewiesen werden.

Auch Art. 12 (5) DSGVO-E stellt keinen redaktionellen Eingriff dar, sondern verschiebt die Funktionslogik eines zentralen Kontrollinstruments. Die Prüfung der subjektiven Zielsetzung eines Auskunftsersuchens ist dem System der DSGVO fremd. Das Auskunftsrecht ist ein Kernbestandteil von Art. 8 GRCh. Es ermöglicht die Kontrolle der Rechtmäßigkeit einer Verarbeitung und ermöglicht die Ausübung weiterer Grundrechte. Die GRCh sieht keine Zweckbegrenzung dieses Rechts vor; es gilt unabhängig vom Motiv einer betroffenen Person. Dementsprechend hat der EuGH mehrfach bestätigt, dass das Auskunftsrecht ein objektives Kontrollinstrument ist und nicht von zusätzlichen Voraussetzungen abhängig gemacht werden darf.[24] Einschränkungen müssen daher den Wesensgehalt des Rechts wahren, verhältnismäßig sein und ein hohes Maß an Rechtssicherheit gewährleisten. Die vorgeschlagenen Änderungen erfüllen diese Anforderungen nicht.

Unbestimmte Begriffe wie „abuse“, „excessive“ oder „overly broad“ erweitern den Ermessensspielraum der Verantwortlichen deutlich und erhöhen das Risiko uneinheitlicher Auslegung. Der gesenkte Beweismaßstab „reasonable grounds to believe“ führt faktisch zu einer Beweislastumkehr zulasten der Betroffenen. Dies ermöglicht pauschale oder automatisierte Ablehnungen ohne substanzielle Prüfung.

Praktische Folgen zeigen sich insbesondere bei datenintensiven Geschäftsmodellen. Anfragen an Auskunfteien dienen etwa häufig dazu, fehlerhafte Bewertungen zu identifizieren und zu korrigieren. Sie können jedoch gleichzeitig legitime wirtschaftliche Interessen verfolgen und nicht ausschließlich den Schutz der eigenen Daten. Die geplante Motivprüfung könnte Verantwortlichen ermöglichen, solche Anfragen als zweckfremd oder missbräuchlich einzustufen – mit erheblichen Auswirkungen auf die Rechte und Freiheiten der Betroffenen.

---

[23] Siehe auch European Data Protection Supervisor: A Preliminary Opinion on data protection and scientific research, 2020, https://www.edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf, 08.12.2025.

[24] Siehe etwa EuGH, Urteil vom 07.03.2024 – 26.10.2023 *FT*; EuGH, Urteil vom 22.06.2023 – C-579/21 *Pankki*

Auch journalistische Recherchen, datenaltruistische Projekte oder zivilgesellschaftliche Untersuchungen – etwa die OpenSchufa-Kampagne[25] oder Analysen systemischer Plattformrisiken[26] – beruhen regelmäßig auf breiten oder wiederholten Ersuchen. Neue, unbestimmte Ablehnungsgründe würden solche Untersuchungen erschweren und die öffentliche Kontrolle eingriffsintensiver Systeme schwächen.

Hinzu kommt: Betroffene können Auskunftsersuchen häufig nicht präzisieren, weil ihnen naturgemäß nicht bekannt ist, welche Daten wie verarbeitet werden. Breite oder wiederholte Ersuchen sind daher etwa bei andauernden Verarbeitungsverfahren, wie Tracking und Profilbildung, bei komplexen Übermittlungen oder bei großen Trainingsdatensätzen unvermeidbar. Die Spezifizierungspflicht schwächt damit die praktische Anwendbarkeit des Auskunftsrechts. Auch Schadenersatzansprüche nach Art. 82 DSGVO könnten mittelbar erschwert werden, wenn fehlende Auskünfte die Darlegung eines Schadens verhindern.

Zudem fehlen stichhaltige Belege, dass das geltende Recht unzureichend wäre, missbräuchliche oder exzessive Ersuchen zurückzuweisen. Die im ErwGr. 35 DO-E genannten Beispiele missbräuchlicher Anfragen fallen bereits heute unter Art. 12 (5) DSGVO. Dass der Erwägungsgrund selbst auf das bestehende Kriterium der Exzessivität verweist, zeigt, dass die geltende Rechtslage die beschriebenen Konstellationen abdeckt. Die vorgeschlagenen Änderungen würden hingegen neue Unklarheiten schaffen und Betroffene mit zusätzlichen Hürden belasten.

> Die geplante Ausweitung der Ablehnungsgründe muss gestrichen werden. Anstatt Rechtsklarheit zu schaffen, würde der Vorschlag gefestigte EuGH-Rechtsprechung infrage stellen, neue Auslegungsunsicherheiten erzeugen und voraussichtlich erneute Klärungsverfahren erfordern. Das Auskunftsrecht muss ohne Motivprüfung und ohne zusätzliche Voraussetzungen anwendbar bleiben.
>
> Eine tatsächliche Klarstellung wäre, Art. 15 (1)(c) DSGVO im Sinne des EuGH-Urteils C-154/21 *Österreichische Post AG* zu präzisieren: Verantwortliche sollten verpflichtet werden, grundsätzlich die konkreten Empfänger einer Datenübermittlung zu benennen. Eine ausdrückliche Bestätigung dieser Rechtsprechung würde Rechtssicherheit und Transparenz stärken, ohne das Auskunftsrecht einzuschränken.

2.2 Zur Abschwächung der Informationspflichten

Neufassung des Art. 13 (4) DSGVO

Die Europäische Kommission will die Ausnahme von den Informationspflichten bei Direkterhebung deutlich erweitern (Art. 3 (5) DO-E). Künftig sollen die Pflichten aus Art. 13 (1) bis (3) DSGVO entfallen, wenn Daten in einem „clear and circumscribed relationship“ erhoben werden, die Tätigkeit des Verantwortlichen „not data intensive“ ist und dieser „reasonable grounds to assume“ hat, dass Betroffene Basisinformationen (Identität, Kontakt, Zweck und Rechtsgrundlage) bereits kennen. Ausgenommen sind lediglich Fälle mit Weitergabe an Dritte, Drittlandübermittlung, automatisierten Entscheidungen oder bei hohem Risiko.

---

[25] https://openschufa.de/

[26] Siehe DSA 40 Data Access Collaboratory: The Amendment to Article 12, paragraph 5 GDPR in the Omnibus Proposal Undermines Evidence-Based Policymaking. Open Letter, 2025, https://dsa40collaboratory.eu/open-letter-omnibus/, 08.12.2025.

Bereits unklar bleibt, welches konkrete Problem diese Neufassung lösen soll. Die Europäische Kommission benennt weder ein Vollzugsdefizit noch empirische Hinweise darauf, dass die bestehenden Transparenzpflichten systematisch zu Überlastung oder unverhältnismäßigem Aufwand führen. Ohne eine belastbare Problemanalyse ist es nicht gerechtfertigt, die zentralen Transparenzpflichten abzusenken.

Die Vorschläge verändern Reichweite und Voraussetzungen der Transparenzpflichten substanziell. Sie ersetzen objektive Kriterien durch Kontextvermutungen und führen neue unbestimmte Rechtsbegriffe sowie eine Kenntnisfiktion ein. Damit verschiebt sich der normative Fokus vom tatsächlichen Informationsstand der Betroffenen zur Einschätzung des Verantwortlichen.

Die Neuregelung stellt keine redaktionelle Präzisierung dar, sondern einen materiellen Eingriff in das Transparenzregime der DSGVO. Das Transparenzgebot ist ein zentrales Element des Grundsatzes „fair and transparent processing“ und Voraussetzung für die Ausübung weiterer Betroffenenrechte. Es ist funktional eng mit Art. 8 GRCh verknüpft; Einschränkungen müssen den Wesensgehalt achten, verhältnismäßig sein und auf klaren, vorhersehbaren Kriterien beruhen. Die vorgeschlagene Neufassung erfüllt diese Anforderungen nicht.

Die Vielzahl unbestimmter Begriffe – etwa „clear and circumscribed relationship“, „not data-intensive“, „low amount of personal data“, „non-complex processing“ und „reasonable grounds to assume“ – schafft erhebliche Auslegungsspielräume. ErwGr. 36 DO-E erweitert die Ausnahme zusätzlich, indem er auf Situationen „not likely to result in a high risk“ abstellt; ein weiter gefasstes Kriterium als im Rechtstext. Dies führt zu struktureller Rechtsunsicherheit, da Begriffe ohne objektive Schwellenwerte durch weitere unbestimmte Begriffe ohne klare Anwendungsgrenzen erläutert werden.

Verantwortliche jeder Größe sollen künftig selbst beurteilen, ob ihre Tätigkeit „not data intensive“ ist, wie eng die Beziehung zu Betroffenen ist, oder ob bei diesen ausreichende Kenntnis angenommen werden kann. Dies erhöht das Risiko fehlerhafter Einstufungen und divergierender Auslegungen in der Praxis. Eine echte Entlastungswirkung entsteht nicht, da die Informationen weiterhin für Rechenschaftspflichten, Auskunftsersuchen und weitere Verarbeitungen vorgehalten werden müssen.

Ferner führt ErwGr. 36 DO-E aus, es sei „reasonable to expect“, dass Betroffene den Zweck der Verarbeitung kennen würden, wenn diese zur Vertragserfüllung oder auf Grundlage einer Einwilligung erfolgt. Der Rechtstext selbst ist jedoch nicht auf diese Rechtsgrundlagen begrenzt. Fehlende Erstinformationen erschweren zudem informierte Einwilligungen nach Art. 4 (11) und Art. 7 DSGVO. Diese setzen voraus, dass Betroffene die maßgeblichen Informationen tatsächlich erhalten. Wenn die Informationen jedoch aufgrund einer Kenntnisfiktion nicht bereitgestellt werden müssen, kann die Einwilligung nicht mehr informiert erfolgen. Die vorgeschlagene Regelung ist daher systematisch widersprüchlich.

Die Kenntnisfiktion schafft Transparenzlücken gerade in alltäglichen Verarbeitungssituationen. Zwar setzt die Ausnahme voraus, dass Verbraucher:innen die Informationen aus Art. 13 (1)(a) und (c) DSGVO bereits kennen sollen. Dennoch entfallen wesentliche weitere Informationen wie Angaben zu berechtigten Interessen, Widerrufsmöglichkeiten, Speicherdauer und Zweckänderungen. Ohne diese Angaben können Betroffene Risiken nicht bewerten und weitere Rechte nicht wirksam ausüben.

Das im ErwGr. 36 DO-E gewählte Beispiel eines Handwerksbetriebs eignet sich nicht als Entlastungsargument. Die Annahme, Verarbeitungen durch Handwerksbetriebe seien, nur weil sie

auf das zur Erbringung der Dienstleistung Erforderliche begrenzt sind, „not data-intensive“ oder „not complex“, ist weder sachlich noch rechtlich tragfähig. Selbst kleine Betriebe können sensible Daten verarbeiten, etwa bei der Installation von Smart-Home-Systemen oder der Reparatur von IT-Geräten mit Zugriff auf private Inhalte.

Die Neufassung geht über eine Klarstellung hinaus und schafft neue materielle Ausnahmebereiche, die das Transparenzprinzip der DSGVO systematisch schwächen. Statt Rechtssicherheit entstehen offene Auslegungsfragen, Vollzugsunsicherheit und eine Absenkung der Erstinformationsqualität.

> Der Gesetzgeber muss die vorgeschlagene Neufassung streichen. Transparenzpflichten müssen auf objektiven Kriterien beruhen und dürfen nicht durch Kontextvermutungen ersetzt werden. Eine Kenntnisfiktion ist mit dem Transparenzgrundsatz und mit Art. 8 GRCh unvereinbar. Sinnvolle Vereinfachungen der Informationspflichten können außerhalb materieller Änderungen der DSGVO erfolgen: Einheitliche Kurztexte und Piktogramme für typische Verarbeitungsvorgänge könnten Unternehmen bei der Erfüllung ihrer Informationspflichten unterstützen und gleichzeitig die Verständlichkeit für Verbraucher:innen erhöhen.[27]

3. Neustrukturierung des Tracking-Schutzes mit Lücken

3.1 Zur Überführung der „Cookie“-Regelungen in die DSGVO

Neuer Art. 88a DSGVO / Änderung des Art. 5 (3) ePrivacy-Richtlinie

Mit Art. 88a DSGVO-E (Art. 3 (15) DO-E) und der flankierenden Änderung von Art. 5 (3) ePrivacy-Richtlinie (Art. 5 DO-E) schlägt die Europäische Kommission eine grundlegende Neuordnung des Endgeräteschutzes vor. Künftig soll der Zugriff auf personenbezogene Daten im Endgerät sowie deren Nutzung grundsätzlich der DSGVO unterliegen. Art. 5 (3) ePrivacy-Richtlinie gilt für natürliche Personen nur noch, wenn der Zugriff nicht zu einer Verarbeitung personenbezogener Daten führt. Sie schlägt ferner weitere Ausnahmen von der Einwilligung vor und verknüpft in ErwGr. 44 DO-E nachfolgende Verarbeitungen mit Art. 6 (1)(f) DSGVO. Zudem führt Art. 88a DSGVO-E eine neue Systematik von Einwilligungsanforderungen ein.

Art. 88a DSGVO-E verlagert den präventiven Schutz des Endgeräts auf die nachgelagerte Verarbeitung. Während Art. 5 (3) ePrivacy-Richtlinie schon Zugriffe unabhängig vom Personenbezug begrenzt, greift die DSGVO erst bei der Verarbeitung personenbezogener Daten. Das steht in deutlicher Spannung zu Art. 7 GRCh. Der Zugriff auf ein Endgerät stellt bereits für sich genommen einen Eingriff in die Privatsphäre dar, unabhängig davon, ob anschließend personenbezogene Daten verarbeitet werden. Fällt der präventive Zugriffsschutz weg, fehlt die Kontrolle an dem Punkt, an dem der Grundrechtseingriff tatsächlich stattfindet. Art. 5 (3) ePrivacy-Richtlinie bliebe nur in seltenen Ausnahmefällen anwendbar, in denen ein Zugriff weder personenbezogene Daten umfasst noch zu einer solchen Verarbeitung führt. Dies ist im Kontext moderner Web- und App-Technologien kaum realistisch.

Demgegenüber würde die geplante Neudefinition personenbezogener Daten im Entwurf zu einem systemischen Widerspruch führen: Viele Gerätedaten würden nicht mehr als personenbezogen

[27] Siehe Verbraucherzentrale Bundesverband (vzbv) (2025) (wie Anm. 7), S. 14.

gelten. Art. 88a DSGVO-E fände dann keine Anwendung, sodass wieder Art. 5 (3) ePrivacy-Richtlinie greifen müsste – mit der Folge, dass für zahlreiche technische Zugriffe weiterhin Einwilligungen erforderlich wären. Damit entstünde die paradoxe Situation, dass Cookie-Banner nicht reduziert, sondern faktisch stabilisiert würden. Die politischen Ziele der Reform würden verfehlt.

Auch die Ausnahmen nach Art. 88a (3) DSGVO-E schaffen erhebliche rechtliche und technische Unsicherheiten und senken das bisherige Schutzniveau. Sie gelten unabhängig von Art. 6 (1) und 9 (2) DSGVO; insbesondere lit. (c) und (d) sind als absolute Ausnahmen formuliert. Dadurch können eingriffsintensive Maßnahmen ohne Abwägung und ohne zusätzliche Schutzmechanismen stattfinden. Die weiten und unbestimmten Ausnahmen genügen damit den Anforderungen des Art. 52 GRCh – insbesondere Vorhersehbarkeit, Notwendigkeit und Präzision – nicht, weil sie weder klar begrenzt noch systematisch eingehegt sind.

So bleibt die Ausnahme zur Reichweitenmessung (lit. (c)) inhaltlich unbestimmt. „Aggregated audience measurement“ wird nicht definiert, insbesondere fehlt eine Festlegung darauf, nach welchen Kriterien Aggregation stattzufinden hat und in welchen Zeiträumen Daten zusammengeführt werden dürfen. Ohne weitere technische Schutzmaßnahmen droht, dass vermeintlich aggregierte Werte re-identifizierbar bleiben. Ohne eine Präzision des Zwecks kann Reichweitenmessung als Deckbegriff für weitreichende Analyse- oder Telemetrieverarbeitungen dienen. Erforderlich wäre außerdem ein jederzeit ausübbares Widerspruchsrecht für Betroffene.

Auch die Sicherheitsausnahme (lit. (d)) ist zu weit gefasst. Unter dem Vorwand der Aufrechterhaltung oder Wiederherstellung der Sicherheit von Diensten oder Geräten sind unangemessen weitreichende Eingriffe möglich. Ohne klare Begrenzung auf Maßnahmen, die der Vertraulichkeit, Integrität und Verfügbarkeit dienen, und ohne zeitliche Einschränkung entstehen erhebliche Risiken. Historische Fälle wie das Sony-Rootkit – bei dem unter dem Vorwand des Kopierschutzes Software heimlich auf Geräten installiert wurde[28] – zeigen, dass „Sicherheits“- oder „Schutz“-Argumente zur Rechtfertigung tiefer und intransparenter Endgerätezugriffe missbraucht werden. Dieser Fall war politisch der zentrale Auslöser dafür, dass Artikel 5(3) ePrivacy-Richtlinie den Zugriff auf Endgeräte strikt und unabhängig vom Personenbezug regelt.

Besonders kritisch ist die geplante Regelung zur Weiterverarbeitung. ErwGr. 44 DO-E nennt ausdrücklich Art. 6 (1)(f) DSGVO als Grundlage für „subsequent processing“. Dies unterläuft die bisherige Systematik des Art. 5 (3) ePrivacy-Richtlinie, die Zugriffe nur bei technischer Erforderlichkeit oder Einwilligung zulässt. Werden Daten, die allein für technische Funktionen, Reichweitenmessung oder Sicherheitsmaßnahmen erhoben wurden, später aber für andere Zwecke genutzt, verliert Zweckbindung ihre Wirkung und es entsteht ein Einfallstor für Profilbildung. Ein ausdrückliches Weiterverarbeitungsverbot ist daher zwingend.

Die vorgesehenen Einwilligungsregelungen lösen zentrale Probleme des Trackings und der Profilbildung[29] kaum und bleiben in ihrer Wirkung begrenzt. Die Möglichkeit, Einwilligungen mit einem einzigen Klick abzulehnen, ist zwar ein Fortschritt, verhindert aber keine Dark Patterns und bleibt hinter der Logik von Art. 7 (3) DSGVO zurück, nachdem der Widerruf der Einwilligung so einfach wie ihre Erteilung sein muss. Auch die sechsmonatige Sperre für erneute Anfragen führt zu paradoxen Effekten: Anbieter müssen den Ablehnungsstatus speichern, was ohne Account

[28] Siehe https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

[29] Siehe auch Verbraucherzentrale Bundesverband: Perspectives for the Regulation of Personalised Advertising, 2025, S. 14ff, https://www.vzbv.de/sites/default/files/2025-02/25-02-10_Positionpaper_vzbv_Personalised-Advertising.pdf, 08.12.2025.

persistente Identifikatoren erfordert und somit den Schutz des Endgeräts schwächt. Löscht eine Person lokale Speicher, entstehen zusätzliche Anfragen – das Gegenteil des angestrebten Effekts.

Zusätzlich fehlt dem Entwurf eine Lösung für Geräte mit mehreren gleichberechtigten Nutzer:innen, etwa Routern, Smart-TVs oder vernetzten Fahrzeugen. Die DSGVO bietet keine Mechanismen, um parallel abgegebene Einwilligungen oder Ablehnungen verschiedener Personen abzubilden. Die präventive Logik der ePrivacy-Richtlinie schützt das Gerät selbst und adressiert diese Konstellationen strukturell. Die Verschiebung zur DSGVO erzeugt hier eine Schutzlücke.

Schließlich erzeugt die Neuregelung widersprüchliche Anreizstrukturen, die ihrem Schutzzweck zuwiderlaufen. Für weniger eingriffsintensive Reichweitenmessungen ohne Personenbezug wäre weiterhin eine Einwilligung nach Art. 5 (3) ePrivacy-Richtlinie erforderlich, während Messungen mit Personenbezug über Art. 88a (3) DSGVO-E zulässig wären. Damit werden eingriffsintensivere Verarbeitungen gegenüber weniger eingriffsintensiven privilegiert.

> Die vorgeschlagene Neustrukturierung muss überarbeitet werden. Der präventive Schutz aus Art. 5 (3) ePrivacy-Richtlinie sollte beibehalten werden. Mindestens aber brauchen die Ausnahmen in Art. 88a (3) klare Zweckgrenzen, technische Mindestanforderungen, ein ausdrückliches Weiterverarbeitungsverbot sowie – für lit. (c) – ein jederzeit ausübbares Widerspruchsrecht. Die Sicherheitsschranke muss präzise gefasst und auf notwendige Maßnahmen begrenzt werden. Dark Patterns müssen ausgeschlossen werden. Um Verbraucher:innen wirksam zu schützen und Unternehmen zu entlasten, wäre es jedoch insgesamt zielführender, Tracking und Profilbildung zu Werbezwecken zu untersagen.[30]

3.2 Zur Einführung automatisierter, maschinenlesbarer Präferenzsignale

Neuer Art. 88b DSGVO

Art. 88b DSGVO-E sieht erstmals ein System automatisierter und maschinenlesbarer Präferenzsignale vor und etabliert damit einen technischen Kernbaustein des neuen Regulierungsrahmens (Art. 3 (15) DO-E). Verantwortliche sollen es Betroffenen ermöglichen, Einwilligungsanfragen automatisiert abzulehnen und Widersprüche nach Art. 21 (2) DSGVO digital auszuüben. Zudem sollen Betroffene Einwilligungen automatisiert erteilen können. Diese Vorgaben sollen jedoch erst greifen, wenn europäische Normungsorganisationen entsprechende Standards entwickelt haben. Browseranbieter sollen technische Möglichkeiten für die Übermittlung solcher Signale bereitstellen, während Medienanbieter von der Pflicht zur Beachtung ausgenommen sind.

Der Ansatz eines maschinenlesbaren Widerspruchs ist sinnvoll. Einheitliche und verbindliche Ablehnungs- und Widerspruchssignale können Betroffenenrechte stärken und die Anzahl manipulativer Einwilligungsbanner reduzieren. Der Vorschlag bleibt jedoch in mehreren Punkten unpräzise und führt zu systemischen Risiken, die das Schutzniveau der DSGVO ohne Nachbesserungen schwächen würden.

Unklar bleibt insbesondere der Anwendungsbereich. Es ist nicht eindeutig, ob Art. 88b DSGVO-E ausschließlich Einwilligungen im Sinne von Art. 88a DSGVO-E betrifft oder sämtliche Einwilligungen der DSGVO. Der Verweis auf „consent under this Regulation“ sowie die Einbindung von Art. 21 (2)

[30] Siehe ebd.

DSGVO sprechen für einen weiten Anwendungsbereich. Nach der Rechtsprechung des EuGH[31] umfasst „Direktwerbung“ jede kommerzielle Ansprache, die sich „direkt und individuell an einen Verbraucher“ richtet, einschließlich personalisierter E-Mails. Die vorgeschlagene Regelung würde also bedeuten, dass Unternehmen über ihre Online-Schnittstellen auch automatisierte Widersprüche gegen individualisierte E-Mails und postalische Direktwerbung akzeptieren müssten. Auch das Verhältnis zu Art. 21 (5) DSGVO bleibt ungeklärt.

Diese Unsicherheit hat praktische Folgen: Verantwortliche wissen nicht, welche Pflichten gelten, und Betroffene können nicht erkennen, wann ihre Entscheidungen wirksam sind. Dies führt zu unterschiedlichen Interpretationen und inkonsistenter Umsetzung, die das Vertrauen in solche Signale untergraben. Außerdem können sich ungewollte Wechselwirkungen mit anderen Rechtsakten – wie etwa dem Digital Markets Act (DMA) – ergeben, die sich auf die Anforderungen der Einwilligung entsprechend der DSGVO beziehen.

Besonders problematisch ist die Möglichkeit, Einwilligungen automatisiert zu erteilen. Eine informierte Einwilligung nach Art. 4 (11) DSGVO setzt voraus, dass Betroffene Zwecke, Risiken, Verantwortliche, Empfänger und Folgen der Verarbeitung kennen und verstehen. Diese Voraussetzungen kann ein globales zentrales Signal systemisch nicht gewährleisten – insbesondere nicht gegenüber dem strukturell intransparenten AdTech-Ökosystem. Auch bleibt der Widerruf von Einwilligungen ungeklärt, obwohl Art. 7 (3) DSGVO verlangt, dass er so einfach sein muss wie die Erteilung. So besteht das Risiko langlebiger, schwer widerrufbarer Zustände. Sachgerecht und technisch tragfähig ist daher allein die automatisierte Ablehnung von Einwilligungsanfragen sowie ein maschinenlesbarer Widerspruch.

Die Pflicht der Anbieter, solche Signale lediglich zu „respektieren“, greift deutlich zu kurz. Notwendig ist eine verbindliche Pflicht zur Befolgung. Die weitreichende Ausnahme für Medienanbieter verstärkt das Problem erheblich. Der Begriff der Mediendiensteanbieter nach der Verordnung (EU) 2024/1083 kann etwa auch große Lifestyle-Seiten, Video- und Streamingdienste sowie Sport- und Entertainmentangebote umfassen. Selbst bei engerer Auslegung – beschränkt auf klassische journalistische Angebote – bliebe die Ausnahme systemwidrig, da besonders diese Angebote zahlreiche Drittinhalte, Werbenetzwerke und Analysedienste einbinden. Die Folge wären schwer nachvollziehbare Parallelregime für große Teile der Informationsangebote im Internet: Während viele datenintensive Dienste Signale ignorieren dürften, müssten andere Anbieter sie befolgen. Dies erschwert informierte Entscheidungen, erzeugt wettbewerbliche Verzerrungen zu Lasten datenschutzfreundlicher Informationsangebote und schafft Anreize und Möglichkeiten, die Regelungen zu umgehen.

Die vorgesehene Standardisierung birgt weitere regulatorische und praktische Risiken. Standards sollen erst entwickelt werden; Fristen fehlen. Währenddessen hätte Art. 88b DSGVO-E keine praktische Wirkung. Dies lässt sich schwer mit dem Anspruch der Reform, kurzfristig Entlastung und Vereinfachung zu schaffen, vereinbaren. Regulatorischer Stillstand wäre eine weitere Folge. Die Möglichkeit, nur Teile eines Standards zu erfüllen und dennoch als konform zu gelten, schafft zusätzliche Risiken und Unsicherheiten. Statt einer Delegation an Standardisierungsorganisationen sollte die Europäische Kommission durch Durchführungsrechtsakte technische Spezifikationen festlegen, um Verzögerungen, industriegetriebene Verwässerung und einen „kleinsten gemeinsamen Nenner“ zu vermeiden. Insbesondere muss sie sicherstellen, dass

[31] Siehe etwa EuGH, Urteil vom 25.11.2021 – C-102/20 *StWL Städtische Werke Lauf a.d. Pegnitz*

- Ablehnungs- und Widerspruchssignale klar erkennbar und eindeutig wirksam sind;
- Verantwortliche keine weiteren Fenster oder Auswahlwege öffnen dürfen, wenn ein aktives Signal vorliegt;
- Browser, Betriebssysteme, Apps und andere digitale Umgebungen einheitliche und interoperable Regeln einhalten;
- Präferenzsignale keine Identifikationsmerkmale bilden und nicht zu persistenten Nutzerkennungen führen;
- ein Ablehnungssignal sämtliche Tracking-Technologien automatisch blockiert, ohne zusätzliche Nutzerinteraktion.

Die Rolle der Browserhersteller ist ambivalent. Einerseits liegt es technisch nahe, Präferenzsignale auf Systemebene zu verankern. Andererseits entsteht eine Machtkonzentration bei wenigen Gatekeepern, die über Voreinstellungen und UI-Design beeinflussen können, welche Präferenzen Betroffene tatsächlich setzen. Da Tracking längst in Apps, Smart-TV-Umgebungen und anderen proprietären Ökosystemen stattfindet, darf die Pflicht nicht auf Browser beschränkt sein. Ohne umfassende Einbeziehung aller Endnutzerumgebungen entstünde eine erhebliche Schutzlücke.

> Der Ansatz maschinenlesbarer Präferenzsignale ist richtig. Diese dürfen jedoch ausschließlich der Ablehnung von Einwilligungsanfragen und dem Widerspruch nach Art. 21 (2) DSGVO dienen. Die Pflicht der Verantwortlichen muss eindeutig und verbindlich ausgestaltet sein, die Ausnahme für Medienanbieter ist systemwidrig und sollte gestrichen werden. Notwendig ist zudem eine technische Spezifikation, die klare semantische Vorgaben, einfache Widerrufsmöglichkeiten, ein wirksames Verbot manipulativer Praktiken und die automatische Blockierung sämtlicher Tracking-Technologien bei aktivem Ablehnungssignal sicherstellt. Browser-, Betriebssystem- und App-Anbieter sowie andere Endnutzerumgebungen sind gleichermaßen einzubeziehen und so zu regulieren, dass ihre Gatekeeper-Position nicht zulasten der Verbraucher:innen wirkt.

4. Unverhältnismäßige Privilegierung der KI-Entwicklung und des -Betriebs[32]

4.1 Zur Ausnahme vom Verarbeitungsverbot sensibler Daten

Neuer Art. 9 (2)(k) DSGVO / neuer Art. 9 (5) DSGVO

Der Vorschlag der Europäischen Kommission sieht eine neue Ausnahme vom Verarbeitungsverbot sensibler Daten vor (Art. 3 (3)(a) DO-E). Nach Art. 9 (2)(k) DSGVO-E sollen sensible Daten für die Entwicklung und den Betrieb von KI-Systemen verarbeitet werden dürfen, sofern der Verantwortliche die in Art. 9 (5) DSGVO-E genannten Voraussetzungen erfüllt. Diese umfassen die Pflicht, geeignete technische und organisatorische Maßnahmen umzusetzen, um die Verarbeitung sensibler Daten zu vermeiden, identifizierte sensible Daten zu entfernen oder – falls deren

[32] Für eine ausführliche Begründung der Positionen dieses Kapitels siehe Hense, Peter; Wagner, David: Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Kontext der Entwicklung und des Einsatzes von KI. Gutachten im Auftrag des vzbv, 2025, https://www.vzbv.de/sites/default/files/2025-12/Gutachten_Hense_Wagner_KI-Rechtsgrundlage.pdf, 12.12.2025.

Entfernung unverhältnismäßigen Aufwand erfordert – diese vor Nutzung, Weitergabe oder Offenlegung wirksam zu schützen (Art. 3 (3)(b) DO-E). Der Anwendungsbereich der Ausnahme beschränkt sich auf residuale Daten – also die Daten, die trotz der Vermeidungsmaßnahmen unbeabsichtigt im Datensatz verbleiben. Zielgerichtete Verarbeitungen sensibler Daten müssen weiterhin auf die bestehenden Tatbestände des Art. 9 (2)(a) bis (j) DSGVO gestützt werden.

Diese Regelung stellt einen systematischen Bruch mit der Grundstruktur der DSGVO dar. Art. 24 DSGVO verpflichtet Verantwortliche, ihre technischen und organisatorischen Maßnahmen risikoadäquat auszugestalten. Je umfangreicher und komplexer die Verarbeitung ausfällt, desto höher müssen die Schutzmaßnahmen sein. Der Entwurf kehrt dieses Verhältnis um, indem er gerade dort eine Privilegierung schafft, wo massenhafte, unstrukturierte und für Betroffene intransparente Datenverarbeitungen stattfinden. Dies senkt das Schutzniveau für besonders eingriffsintensive Verarbeitungen und unterläuft die risikobasierte Logik der DSGVO.

Hinzu kommt ein deutlicher Konflikt mit der EuGH-Rechtsprechung zu Art. 9 (1) DSGVO. Der Gerichtshof hat mehrfach klargestellt, dass bereits ein einziges sensibles Datum in einem Datensatz dazu führt, dass die gesamte Verarbeitung dem Verbot des Art. 9 (1) DSGVO unterfällt – unabhängig von der Absicht des Verantwortlichen.[33] Der Vorschlag der Europäischen Kommission privilegiert jedoch die untrennbare Vermischung sensibler und nicht-sensibler Daten und macht sie zur Grundlage einer neuen Ausnahme. Diese Konstruktion wirft daher erhebliche Zweifel an der unionsrechtlichen Tragfähigkeit des Vorschlags auf.

Problematisch ist zudem, dass Betroffene faktisch den Anknüpfungspunkt für Rechtsbehelfe verlieren. Wird die Verarbeitung sensibler Daten durch Art. 9 (2)(k) DSGVO-E privilegiert, liegt kein Verstoß gegen Art. 9 (1) DSGVO vor. Damit entfällt insbesondere der Schutz bei Kontrollverlusten, die der EuGH als immateriellen Schaden anerkennt. Die Ausnahme nimmt Verantwortliche damit aus der haftungsrechtlichen Verantwortung, ohne den Betroffenen ein alternatives, wirksames Schutzinstrument oder einen angemessenen Ausgleich zur Verfügung zu stellen.

Der Vorschlag übernimmt die vom OLG Köln entwickelte Logik einer „tätigkeitsbezogenen Reduktion“ des Art. 9 DSGVO.[34] Danach greift das Verarbeitungsverbot bei massenhaft automatisierter Datenverarbeitung faktisch erst, wenn Betroffene aktiv werden. Diese Logik überzeugt im Kontext des KI-Trainings nicht. Betroffene wissen nicht, dass ihre Daten genutzt werden, können nachträglich nicht widersprechen und auch keine Entfernung verlangen. Art. 9 (5) DSGVO-E akzeptiert, dass sensible Daten im System verbleiben, und verlagert den Schutz auf nachgelagerte Maßnahmen wie Output-Filterung. So entsteht ein erhebliches Spannungsverhältnis zur jüngsten EuGH-Rechtsprechung in der Rechtssache C-492/23 *Russmedia*, die proaktive Prüfpflichten bei sensiblen Daten betont und nachträgliche Korrekturen nicht ausreichen lässt.

Schwer wiegt auch die Aufweichung des Erforderlichkeitsgrundsatzes. Art. 9 (5) DSGVO-E erlaubt die Verarbeitung sensibler Daten, die für die Zwecke der KI-Entwicklung nicht erforderlich sind, sofern sie trotz Vermeidungsmaßnahmen im Datensatz verbleiben. Diese Konstruktion widerspricht dem Grundsatz der Datenminimierung in Art. 5 (1)(c) DSGVO und droht, über ErwGr. 30 und 31 auch die Anwendung des Art. 6 (1)(f) DSGVO zu verschieben. Der Entwurf stellt das KI-Training dort pauschal als berechtigtes Interesse dar und legt damit nahe, dass die Verarbeitung großer, auch irrelevanter Datenmengen typischerweise als erforderlich gelten könne. Dies unterläuft die vom

---

[33] Siehe etwa EuGH, Urteil vom 04.07.2023 – C-252/21 *Meta/Bundeskartellamt*

[34] OLG Köln, Urteil vom 23.05.2025 – 15 UKl 2/25.

EuGH entwickelten Maßstäbe:[35] Ein berechtigtes Interesse trägt nur, wenn das verfolgte Ziel nicht durch weniger eingriffsintensive Mittel erreichbar ist. Der Entwurf lässt eine solche Prüfung vermissen und senkt damit das Schutzniveau zulasten der Betroffenen.

In der Gesamtschau führt Art. 9 (2)(k) DSGVO-E zu einer spürbaren Absenkung des Schutzes sensibler Daten, widerspricht zentralen Leitentscheidungen des EuGH und schwächt den Grundsatz proaktiver Schutzmechanismen. Die vorgeschlagene Ausnahme birgt erhebliche rechtliche und grundrechtliche Risiken und ist kein tragfähiger Bestandteil eines kohärenten europäischen Datenschutzniveaus.

> Art. 9 (2)(k) DSGVO-E muss gestrichen werden. Verantwortliche sollten auf die bestehenden, eng umrissenen Ausnahmetatbestände des Art. 9 (2)(a) bis (j) DSGVO verwiesen werden, die ein ausgewogenes und grundrechtlich tragfähiges Schutzniveau gewährleisten.

4.2 Zur Rechtsgrundlage für KI-Entwicklung und -Betrieb

Neuer Art. 88c DSGVO

Der Vorschlag der Europäischen Kommission sieht mit Art. 88c DSGVO-E eine Konkretisierung von Art. 6 (1)(f) DSGVO für Verarbeitungen vor, die „in the context of the development and operation“ von KI-Systemen stattfinden (Art. 3 (15) DO-E). Die Norm schafft keine eigenständige Rechtsgrundlage, sondern beschreibt, dass solche Verarbeitungen auf ein berechtigtes Interesse gestützt werden können, und verweist auf die dabei zu berücksichtigenden Anforderungen des Art. 6 (1)(f) DSGVO. Ergänzend nennt Art. 88c DSGVO-E bestimmte „angemessene“ Schutzmechanismen, darunter die Datenminimierung, den Schutz vor Offenlegung residualer Daten, „enhanced transparency“, ein unbedingtes Widerspruchsrecht sowie einen Hinweis auf die Schutzbedürftigkeit von Kindern.

Unabhängig des Vorschlags kann bereits heute das KI-Training grundsätzlich auf ein berechtigtes Interesse nach Art. 6 (1)(f) DSGVO gestützt werden, sofern dieses Interesse rechtmäßig ist und die Interessen oder Grundrechte der Betroffenen nicht überwiegen. Der EDSA bestätigt dies und betont zugleich die enge Erforderlichkeitsprüfung, wonach eine Verarbeitung nur zulässig ist, wenn das verfolgte Ziel nicht durch weniger eingriffsintensive Mittel erreicht werden kann.[36] Um die Rechtssicherheit zu stärken und Klarheit herbeizuführen, sollte eine darüberhinausgehende gesetzliche Konkretisierung verbindliche materielle Schutzstandards festlegen, um einen unionsweit einheitlichen Mindestschutz zu gewährleisten und gleiche Wettbewerbsbedingungen zu schaffen. Dafür ist erforderlich, dass eine solche Konkretisierung klar formulierte Anforderungen enthält und sich nicht in unverbindlichen Absichtserklärungen erschöpft.

Die Übernahme des Systembegriffs aus Art. 3 (1) KI-Verordnung[37] führt jedoch zu einem faktisch grenzenlosen Sonderregime. Da der KI-Begriff nahezu jede Form automatisierter Datenverarbeitung

---

[35] Siehe etwa EuGH, Urteil vom 09.01.2025 – C-394/23 *Mousse*.

[36] Siehe European Data Protection Board: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 2024, Rn. 64, https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf, 08.12.2025.

[37] „KI-System“ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele

umfasst, entsteht ein Anwendungsbereich, der nicht auf echte KI-Modelle oder modellbasierte Lernprozesse beschränkt ist, sondern potenziell sämtliche datengetriebene Systeme einschließt. Die Formulierung „in the context of the development and operation“ sowie die Bezugnahme in ErwGr. 30 auf die „use“-Phase verstärken dies, indem jede mittelbare Nutzung eines Modells oder Systems erfasst wird. Die Integration eines statischen, systembasierten Begriffs aus dem KI-Recht in einen prozess- und risikobasierten datenschutzrechtlichen Rahmen kollidiert mit der Grundlogik der DSGVO: Diese bewertet konkrete Verarbeitungsvorgänge, nicht abstrakte Systemeinheiten. Ohne klare technische und regulatorische Systemgrenzen ist jedoch keine belastbare Risikobewertung möglich. Dies unterläuft die Anforderungen aus Art. 24 und 25 DSGVO und führt nicht zu mehr Rechtssicherheit, sondern zu struktureller Intransparenz und einer erheblichen Absenkung des Schutzniveaus nach Art. 7 und 8 GRCh.

Art. 88c DSGVO-E benennt zwar zusätzliche Anforderungen wie Datenminimierung, Schutz vor Offenlegung residualer Daten sowie besondere Rücksicht auf Kinder, bleibt jedoch in zentralen Punkten unbestimmt. Begriffe wie „appropriate measures“ werden nicht konkretisiert, während der EDSA präzise Maßnahmen[38] fordert. Die fehlende Konkretisierung erschwert Kontrolle und widerspricht dem Grundsatz der Datenminimierung. Auch das unbedingte Widerspruchsrecht wird nur rudimentär erwähnt, ohne Vorgaben zu dessen praktischer Umsetzung, etwa hinsichtlich Fristen, Dokumentationspflichten, der Einbeziehung Dritter ohne Nutzerkonto oder spezifischer Lösch- und Rücknahmevorgaben für bereits verarbeitete Daten. Da Trainingsdaten irreversibel in Modelle einfließen können und generative Modelle Inhalte reproduzieren, genügt ein rein für künftige Verarbeitungsvorgänge gültiges Widerspruchsrecht nicht; ohne klare Verpflichtungen zur Entfernung bereits genutzter Daten bleibt dieses Recht wirkungslos. Das Widerspruchsrecht bietet außerdem keinen wirksamen Schutz, wenn KI-Modelle als Open Source veröffentlicht werden, da nachträgliche Widersprüche oder Löschungsanträge gegenüber dem ursprünglichen Verantwortlichen wirkungslos bleiben, sobald das Modell frei verfügbar und unkontrollierbar verbreitet ist. Auch wird in Art. 88c DSGVO-E zwar das besondere Schutzbedürfnis von Kindern erwähnt, jedoch ohne konkrete Vorgaben. Da personenbezogene Daten Minderjähriger auch durch Dritte online gestellt werden und ohne Zutun der Betroffenen ins KI-Training einfließen können, greift der bloße Hinweis zu kurz.

Schutzmechanismen werden im Entwurf überwiegend in die Erwägungsgründe verlagert. ErwGr. 31 fordert etwa technische Opt-out-Signale wie robots.txt, die jedoch ausschließlich Betreiber:innen von Webseiten einrichten können. Für Nutzer:innen großer Plattformen und Social-Media-Dienste bietet dieser Ansatz keinen Schutz und erzeugt lediglich die Erwartung formaler, aber materiell irrelevanter Maßnahmen. Die Erwägungsgründe greifen zwar einzelne weitere Elemente aus den Empfehlungen des EDSA auf, formulieren sie jedoch so unbestimmt, dass sie in der Praxis leerzulaufen drohen. Dies gilt insbesondere für „enhanced transparency“,[39] das ohne konkrete Anforderungen zu fragmentierten oder marketingorientierten Informationsformaten führen wird.

Systematisch problematisch sind die Bewertungsmaßstäbe in ErwGr. 31. Die Einführung des Kriteriums, ob ein Interesse „beneficial for the data subject and society at large“ sei, verschiebt die Abwägung zugunsten abstrakter Gemeinwohlbehauptungen und zulasten einer präzisen

---

ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

[38] Siehe European Data Protection Board (EDPB) (2024) (wie Anm. 36), Rn. 51 f., 58, 105.

[39] Siehe ebd., Rn. 103.

Risikobetrachtung. Für Grundlagenmodelle, deren konkrete Verwendung den Verantwortlichen selbst nicht bekannt ist, ist eine solche Prüfung ohnehin faktisch unmöglich. Auch das Kriterium der „reasonable expectations“ ist strukturell verzerrt: Es privilegiert große Plattformen mit bestehender Nutzerbasis, da nur in bestehenden Beziehungen Erwartungen entstehen können. Auch bietet es keine Schutzmechanismen gegen rückwirkende Erwartungskonstruktionen.

Zusammenfassend zeigt sich, dass Art. 88c DSGVO-E die strukturellen Defizite der bisherigen Rechtsprechung nicht adressiert[40] – insbesondere die fehlende Wirksamkeit von Widerspruchs- und Auslistungsmechanismen sowie die Schutzlosstellung nichtregistrierter Dritter. Auch zentrale Vorgaben des EuGH zur Erforderlichkeitsprüfung, zur Zweckbindung und zur Transparenz bleiben unberücksichtigt. Damit gelingt es der Norm nicht, die Anforderungen des Art. 6 (1)(f) DSGVO zu präzisieren oder die Abwägungsstrukturen operabel zu gestalten. Stattdessen verschiebt der Entwurf die Interessenabwägung systematisch zugunsten der Verantwortlichen, ohne die mit datenintensiven KI-Entwicklungen verbundenen Risiken für Betroffene angemessen zu erfassen. Vor diesem Hintergrund entsteht kein kohärentes, risikoadäquates Schutzregime, sondern ein faktisch grenzenloses Sonderregime für KI-bezogene Verarbeitungen, dessen unbestimmte Anforderungen zu Rechtsunsicherheit, zu Scheinschutzmechanismen und zu einer strukturellen Absenkung des Datenschutzniveaus führen.

Auch bei einer Beschränkung der Vorschläge auf reines KI-Training bleibt zweifelhaft, dass eine bloße Modifikation der Interessenabwägung in Art. 6 (1)(f) DSGVO den besonderen Risiken dieser Verarbeitungen gerecht werden könnte. Da KI-Training sich grundlegend von herkömmlichen Verarbeitungen unterscheidet – irreversible Integration von Daten in Modelle, fehlende Löschbarkeit und mögliche Reproduktion in Ausgaben – wird deutlich, dass eine Anpassung der bestehenden Abwägungsstrukturen diesen Besonderheiten nicht gerecht wird.

> Die Verarbeitung personenbezogener Daten für das KI-Training erfordert eine eigenständige Rechtsgrundlage mit strengen materiellen Voraussetzungen:[41] Hierfür erforderlich ist ein Nachweis der Subsidiarität gegenüber synthetischen oder anonymisierten Daten, eine spezifische Risikoinformation vor Beginn der Verarbeitung, ein wirksames Widerspruchsrecht auch für Dritte ohne Nutzerkonto, klare technische Schutzmaßnahmen gegen Reproduktion und Identifizierbarkeit sowie ein Einwilligungserfordernis für Daten von Kindern.[42]

[40] Etwa wie die Widersprüche zwischen OLG Köln, Urteil vom 23.05.2025 – 15 UKl 2/25 sowie OLG Schleswig, Urteil vom 12.08.2025 – 6 UKl 3/25; siehe Hense, Peter; Wagner, David (2025) (wie Anm. 32), S. 6f.

[41] Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich, 2025, https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_DSGVO_KI_Anpassungen.pdf, 12.12.2025.

[42] Für einen Formulierungsvorschlag siehe Hense, Peter; Wagner, David (2025) (wie Anm. 32), S. 26f.

Impressum

Herausgegeben von:
Verbraucherzentrale Bundesverband e.V.
Team Digitales und Medien
Rudi-Dutschke-Straße 17, 10969 Berlin

T +49 30 25800-0
digitales@vzbv.de
vzbv.de

Der Verbraucherzentrale Bundesverband e.V. ist im Deutschen Lobbyregister und im europäischen Transparenzregister registriert. Sie erreichen die entsprechenden Einträge hier und hier.