IMPULSE
für die Wirtschaftspolitik

Reformimpulse für den EU-Regulierungsrahmen zur Stärkung von Wettbewerb und Innovation im Kontext Künstlicher Intelligenz und Daten

Studie im Auftrag der IHK für München und Oberbayern

IHK München und Oberbayern

Technische Universität München

Wirtschaft für Zukunft

IMPULSPAPIER

„Reformimpulse für den EU-Regulierungsrahmen zur Stärkung von Wettbewerb und Innovation im Kontext Künstlicher Intelligenz und Daten“

erstellt durch
Prof. Dr. Boris Paal, M.Jur. (Oxford)
Inhaber des Lehrstuhls für Law and Regulation of the Digital Transformation,
Leiter der Arbeitsgruppe Datenrecht am TUM Think Tank,
Technische Universität München

im Auftrag der
Industrie- und Handelskammer für München und Oberbayern (IHK)

im
Juni 2026

Das vorliegende Dokument ist unabhängig und unparteiisch erstellt worden auf der Grundlage einer sorgfältigen Analyse des geltenden Rechts, der dazu ergangenen Gerichts- und Behördenentscheidungen sowie des einschlägigen Schrifttums.

Inhaltsverzeichnis

Executive Summary

Unternehmen, die KI entwickeln und einsetzen wollen, sind mit erheblichen Rechtsunsicherheiten belastet. Diese Rechtsunsicherheiten haben signifikante unmittelbare wirtschaftliche und strategische Konsequenzen mit weitreichenden Implikationen für grundrechtlich geschützte Positionen der Unternehmen. Vor dem Hintergrund des laufenden europäischen Digital Omnibus-Reformprozesses und des bevorstehenden Digital Fitness Checks zur Nachjustierung des europäischen Digital Acquis besteht die Möglichkeit und Chance, diese Rechtsunsicherheiten zu adressieren und durch gezielte Modifikationen möglichst weitgehend auszuräumen.

In diesem Zusammenhang ist auch und gerade die Datenschutz-Grundverordnung (DSGVO) in den Blick zu nehmen, die mit dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein fundamentales Grundrecht sichert (Art. 8 Grundrechte-Charta – GRCh). Zugleich schadet jedoch die aktuelle Auslegungs- und Durchsetzungspraxis der DSGVO sowie zusammenhängender Digitalrechtsakte sowohl dem Datenschutz als auch den allgemein anerkannten Zielen Innovation und Wettbewerbsfähigkeit.

Ein Null-Risiko-Ansatz bei der Auslegung und Anwendung der DSGVO ist weder (grund-)rechtlich geboten noch zielführend. Das Datenschutzgrundrecht aus Art. 8 GRCh ist kein absolutes Recht, sondern in eine Interessen- und Grundrechtsabwägung am Verhältnismäßigkeitsmaßstab und zur Herstellung von praktischer Konkordanz einzustellen. Zur normativen Absicherung der erforderlichen Abwägung empfiehlt sich die Statuierung eines Innovationsmandats für Aufsichtsbehörden.

Der risikobasierte Ansatz für Rechtsauslegung und -anwendung muss normativ (stärker) verankert werden. Als tragendes Strukturprinzip ist der risikobasierte Ansatz (im Sinne von Verhältnismäßigkeit und praktischer Konkordanz) in der DSGVO angelegt, wird aber bislang nicht konsequent genug aktiviert. *De lege ferenda* sind diese Grundsätze daher ausdrücklich im Normtext festzuschreiben.

Training und Einsatz von KI sind auf berechtigte Interessen stützbar. Art. 6 Abs.1 lit. f) DSGVO (Interessenabwägung) ist grundsätzlich eine taugliche Rechtsgrundlage für die betreffenden Datenverarbeitungen. Die Einwilligung ist keine privilegierte oder vorrangige Rechtsgrundlage. Technische Schutzmaßnahmen (z.B. Differential Privacy und Pseudonymisierung) senken das Risiko und sind positive Faktoren für die Abwägung. In diesem Sinne stehen vereinzelte Personenbezüge in Mischdatensätzen einem auf Art. 6 Abs.1 lit. f) DSGVO gestützten KI-Training auch und gerade dann

nicht entgegen, wenn das Risiko für die betroffenen Personen durch entsprechende Schutzmaßnahmen entscheidend gesenkt wird.

Kumulative Compliance-Lasten müssen abgebaut werden. Das Nebeneinander von DSGVO und anderen Digitalrechtsakten, wie etwa dem Data Act, ist für Unternehmen kaum (mehr) beherrschbar. Widersprüche und Inkohärenzen sind zu beseitigen. Hierzu sind auch praktisch rechtssicher umsetzbare Leitlinien und Orientierungshilfen erforderlich.

Auslegungshoheit ist die entscheidende institutionelle Stellschraube. Es empfiehlt sich eine Übertragung der Auslegungshoheit auf die EU-Kommission durch Erweiterung ihrer Durchführungsbefugnisse als gerichtlich überprüfbares Gegenmodell zum bestehenden Regime des Europäischen Datenschutzausschusses (EDSA).

Rechtliche Analyse und Reformperspektiven

Die aktuellen Diskussionen zur Verbesserung der Innovationskraft, Wettbewerbsfähigkeit und Souveränität Europas im Zeichen der digitalen Transformation verdeutlichen einen erheblichen Handlungs- und Reformbedarf. Dieser Reformbedarf betrifft auch und gerade die Anpassung der rechtlichen Rahmenbedingungen. Europa steht vor der strategischen Herausforderung, Grundrechtsschutz und Regulierung, Innovations- und Wettbewerbsfähigkeit in Einklang zu bringen. Hierbei wird es vor allem auch darauf ankommen, regulatorische Exzellenz mit technologischer Innovationskraft zu verbinden. Es ist ein Umfeld zu schaffen, in dem Wissenschaft, Start-ups, Mittelstand und globale Unternehmen datenbasierte Wertschöpfung verantwortungsvoll und wettbewerbsfähig realisieren können. An dieser Stelle setzt das vorliegende Impulspapier an und arbeitet heraus, welche regulatorischen Stellschrauben mit Blick auf Daten und spezifisch die DSGVO anzupassen sind, um die Nutzung und Entwicklung von KI in und durch Unternehmen zu fördern.

Dies geschieht vor dem Hintergrund, dass sich das europäische Daten(schutz)recht in einer Phase intensiver Reformdiskussionen befindet. Der Digital Omnibus der EU-Kommission vom November 2025 und der sich hieran unmittelbar anschließende Digital Fitness Check eröffnen konkrete Fenster für Reformimpulse und Veränderungen,[1] auch und gerade betreffend die lange Zeit als faktisch „unantastbar“ angesehene DSGVO. Dem liegt die Einsicht zugrunde, dass Daten eine zentrale Ressource für KI und die digitale Transformation sind, wobei ein Großteil der Daten einen Personenbezug aufweist – und damit die DSGVO zur Anwendung berufen ist.

Das Impulspapier adressiert und integriert die laufende Reformdiskussion, wobei auf ihrer Grundlage konsolidierte Handlungsempfehlungen für Innovation, Wachstum und Wettbewerb entwickelt werden – auch und gerade um für Unternehmen bessere KI-Rahmenbedingungen durch Rechtssicherheit und Vereinfachung zu gewährleisten.

(Haupt-)Ziel des Impulspapiers ist die Erarbeitung konkreter Vorschläge zur strategischen Weiterentwicklung des europäischen Digital Acquis, um die Entwicklung und Nutzung von KI in Unternehmen zu unterstützen und damit die zentrale Leitfrage dieser Untersuchung zu beantworten: „Wo müssen wir mit Blick auf das Datenrecht ansetzen, um die Nutzung und Entwicklung von KI in Unternehmen rechtssicher und grundrechtskonform zu ermöglichen?“

---

[1] Eine Übersicht präsentieren *Dose/Pühl*, RDi 2026, 122 ff.

A. Regulierungsrahmen als Wettbewerbs- und Innovationshemmnis

Die EU hat mit der Datenschutz-Grundverordnung (DSGVO), dem Data Governance Act (DGA), dem Data Act (DA), dem Digital Markets Act (DMA), dem Digital Services Act (DSA) und der KI-Verordnung (KI-VO) sowie weiteren Digitalrechtsakten einen ebenso umfassenden wie komplexen, leider aber nicht durchgängig kohärenten und in der praktischen Umsetzung herausfordernden Digital Acquis etabliert. Diese Komplexität in Verbindung mit sich teilweise widersprechenden Vorgaben erschwert Unternehmen den rechtssicheren Einsatz bzw. die Entwicklung von KI unter Nutzung von Daten sowie die Entwicklung und Umsetzung von geeigneten Compliance-Maßnahmen.

Die Herstellung von Kohärenz und Harmonisierung innerhalb des europäischen Digital Acquis ist keine bloß rechtspolitische Forderung, sondern vielmehr eine funktionale Grundvoraussetzung, damit (nicht nur) Unternehmen die Möglichkeiten der KI-Nutzung und -Entwicklung wirksam und rechtssicher ausschöpfen können. Fragmentierung, Inkohärenzen und Widersprüche zwischen DSGVO, KI-VO und weiteren Digitalrechtsakten erzeugen kumulative Compliance-Lasten, die über die Belastungen durch die einzelnen Regelwerke weit hinausgehen.

I. Das datenpolitische Reformfenster: Digital Omnibus und Digital Fitness Check

Europa befindet sich in einem günstigen datenpolitischen Reformmoment, in dem ein Fenster für umfassende Veränderungen zur Förderung von Innovation und Wettbewerbsfähigkeit besteht. Am 19. November 2025 hat die EU-Kommission ein Digitalpaket vorgelegt, das die bestehenden Vorschriften für KI, Cybersicherheit und Daten straffen und überarbeiten soll.[2] Dies geschah mit dem erklärten Ziel, Vereinfachung und Entbürokratisierung zugunsten von Innovation zu stärken.

Am 7. Mai 2026 kam es zu einer Einigung im Trilog-Verfahren zum Digital Omnibus mit Blick auf die KI-Regulierung.[3] Die Stoßrichtung des ursprünglichen Kommissionsvorschlags wird hierbei grundsätzlich beibehalten. Mithin bleibt der materielle Kern der KI-VO unverändert, während zugleich das Zusammenspiel mit

---

[2] COM(2025) 837.

[3] Vgl. die Pressemitteilung vom 7. Mai 2026: online abrufbar: https://www.consilium.europa.eu/de/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/. Siehe den Entwurf aus dem Trilog Council of the European Union, 9247/26, online abrufbar: https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf.

sektorspezifischen Rechtsakten neu justiert wird, Umsetzungsfristen verlängert[4] und Meldeanforderungen konzentriert sowie vereinfacht werden.

Parallel hat die EU-Kommission einen Digital Fitness Check eingeleitet,[5] um zu prüfen, wie bestehende Regelungsregime im Digitalbereich zusammenwirken, welche Belastungen der Digital Acquis für Unternehmen bringt und in welchen Bereichen Überschneidungen, Widersprüche oder unnötige Verwaltungsaufwände bestehen. Der Digital Fitness Check ist das Verfahrensfenster für strukturelle Reformen, die der Digital Omnibus (noch) nicht adressiert, wobei gerade die Kohärenz der verschiedenen Digital- und Datenrechtsakte im Vordergrund stehen soll. Darüber hinaus sollte mittel- und langfristig darauf hingearbeitet werden, eine (risikobasierte) Output-Regulierung in den Vordergrund zu stellen, statt weiterhin auf die derzeitige Input-Regulierung zu setzen.[6]

II. Ausgangslage: Europas digitale Wettbewerbsposition

Europa steht bei der Gestaltung seiner digitalen Zukunft vor großen Herausforderungen. Die europäische Regulierungslandschaft im Digitalbereich ist ausgesprochen komplex, mit sich überschneidenden und teilweise widersprechenden Vorgaben. Der Befund ist ernüchternd: Im globalen Wettbewerb um die Technologieführerschaft bei KI positionieren sich die USA mit massiven staatlichen Investitionsprogrammen,[7] China mit strategischen Industriepolitikmaßnahmen[8] und zentralisiertem Datenzugang[9], Indien und der Nahe Osten mit gezielter Standortpolitik.[10] Zugleich droht Europa aufgrund der Komplexität seines Digital

---

[4] Siehe auch die Forderung der Kommission „Wettbewerb & Künstliche Intelligenz“, KI, Wettbewerb & Wettbewerbsfähigkeit, 2026, S. 129 ff.
[5] Ares(2025)10018469.
[6] Kommission „Wettbewerb & Künstliche Intelligenz“, KI, Wettbewerb & Wettbewerbsfähigkeit, 2026, S. 83 f.
[7] Statt vieler *Borges/Deng*, Innovation Lightbulb: Federal R&D Funding Matters for U.S. AI Leadership, 22.10.2025, online abrufbar: https://www.csis.org/blogs/innovation-lightbulb-federal-rd-funding-matters-us-ai-leadership; *Taufer* et. al., Now More Than Ever, Foundational AI Research and Infrastructure Depends on the Federal Government, 2024-2025, online abrufbar: https://arxiv.org/pdf/2506.14679. Zum „AI Action Plan“ der Trump-Regierung *Spies*, KIR 2025, 284 f.
[8] Zur chinesischen Gesetzgebung bezogen auf KI *Qu*, RDi 2026, 112 ff., Rn. 3 ff.
[9] *Ferner*, Überblick über die Regulierung von Künstlicher Intelligenz (KI) in China, 18.05.2024, online abrufbar: https://www.ferner-alsdorf.de/ueberblick-ueber-die-regulierung-von-kuenstlicher-intelligenz-ki-in-china/.
[10] Zu Indien: *trendreport*, Indiens KI-Ambition zwischen Aufbruch und Risiko, 23.02.2026, online abrufbar: https://www.csis.org/blogs/innovation-lightbulb-federal-rd-funding-matters-us-ai-leadership; *Wenke*, Indien geht es bei künstlicher Intelligenz um Entwicklung, 03.11.2025, online abrufbar: https://www.gtai.de/de/trade/indien/specials/ki-strategie-1901906. Zum Nahen Osten: *Cory* et. al., The Middle East’s Big Bet on Artificial Intelligence and Data Security, 24.09.2025, online abrufbar: https://www.crowell.com/en/insights/client-alerts/the-middle-easts-big-bet-on-artificial-intelligence-and-data-security; *Leitner Cohen*, AI regulations in the Middle East: a hotbed of innovation, 02.12.2024, online abrufbar: https://gcore.com/blog/ai-regulations-2024-middle-east; *Soliman*, From Crude to

Acquis den Anschluss an maßgebliche technologische Entwicklungen zu verlieren. Konkret verursachen aus der DSGVO abgeleitete Einschränkungen bei der Erhebung, Speicherung und Verarbeitung personenbezogener Daten hohe Compliance-Lasten.[11] Diese Compliance-Lasten erschweren das Training sowie die Nutzung von KI-Modellen und stellen für EU-Unternehmen im internationalen Wettbewerb einen gravierenden Standortnachteil dar.

Zudem belegt eine fragmentierte Aufsichtsstruktur mit divergierenden Auslegungsstandards, dass der Harmonisierungsanspruch der DSGVO bislang allenfalls bedingt eingelöst wurde.[12] Insoweit schadet der Status quo somit sowohl dem Datenschutz (durch mangelnde Effizienz der Durchsetzung) als auch der Innovations- und Wettbewerbsfähigkeit (durch mangelnde Rechtssicherheit).[13]

Bereits im Ausgangspunkt ist dabei festzuhalten, dass Regulierung und Innovationsförderung gerade keine natürlichen Gegensätze darstellen (müssen). Vielmehr sind Rechtsunsicherheit und fehlende Vorhersehbarkeit die größten Hemmnisse für Innovation. In diesem Sinne kommt es darauf an, durch eine gelungene Balance von unterschiedlichen (Grund-)Rechtspositionen und Interessen einen angemessenen Ausgleich im Sinne einer praktischen Konkordanz herzustellen, um ein ausreichendes Datenschutzniveau mit Innovation und Wettbewerbsfähigkeit zu verbinden.

III. Draghi-Report (2024): Bestandsaufnahme und Befund sowie weitere Perspektiven

Der Draghi-Report „The Future of European Competitiveness“ aus dem Jahr 2024[14] stellt der EU-Wettbewerbsfähigkeit ein ernüchterndes Zeugnis aus. Obwohl der Bericht die ambitionierten Ziele der DSGVO dem Grunde nach positiv hervorhebt, wird mit guten Gründen festgehalten, dass die nationale Fragmentierung und die Anwendung von EU-Vorgaben auf Sachverhalte, die gar nicht genuiner Gegenstand der EU-Vorgaben sind („Gold-Plating“) bei der Umsetzung der DSGVO sowie die Komplexität

---

Compute: Building the GCC AI Stack, 10.12.2025, online abrufbar: https://mei.edu/publication/from-crude-to-compute-building-the-gcc-ai-stack/.

[11] *Demirer/Hernández/Li/Peng*, DATA, PRIVACY LAWS AND FIRM PRODUCTION: EVIDENCE FROM THE GDPR, Feb. 2026, OA-10 ff., online abrufbar: https://www.nber.org/system/files/working_papers/w32146/w32146.pdf.

[12] *Engelmann*, ZD 2026, 250, 251; *Federmann*, CCZ 2025, 101, 107.

[13] So auch schon Kommission Wettbewerbsrecht 4.0, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, 2019, S. 84, abrufbar unter https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=3.

[14] *Draghi*, The Future of European Competitiveness, 2024, online abrufbar: https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059.

und das Risiko von Überschneidungen und Unstimmigkeiten zwischen den verschiedenen Rechtsakten die Anstrengungen und Zielsetzungen im Rahmen der digitalen Transformation zu untergraben drohen. Der Draghi-Report benennt zutreffend die Koexistenz von rund 100 auf den Digitalsektor bezogenen Gesetzen und mehr als 270 Regulierungsbehörden,[15] wobei die Zahlen seit dem Jahr 2024 weiter angestiegen sind.

Konkret identifiziert der Draghi-Report folgende Kerndefizite:

- Fragmentierte Rechtsdurchsetzung und Rechtsunsicherheit[16]: Aufsichtsbehörden legen zentrale Begriffe (wie etwa berechtigtes Interesse, Zweckkompatibilität, Risikobewertung) unterschiedlich aus.
- Compliance-Last[17]: Die Pflichtendichte trifft vor allem KMU stark und wird zunehmend als Ausdruck einer nachteiligen Überregulierung wahrgenommen.
- Innovationsfeindliche Risikokultur[18]: Eine überstrenge Auslegung der DSGVO („Gold-Plating“) führt zu einer Kultur der Risikoaversion, weshalb Unternehmen bestimmte Technologien nicht entwickeln bzw. zur Anwendung bringen.
- Investitionshemmnis[19]: EU-Unternehmen sind weniger bereit, in Forschung und Entwicklung zu investieren, was die EU hinter Wettbewerber (vor allem) aus USA und China zurückfallen lässt.

Aus strukturanalytischer Perspektive sind zudem drei spezifisch deutsche Faktoren zu benennen, die die europaweit diskutierten Defizite noch verschärfen: (1) eine historisch gewachsene Sonderrolle, die sich deutsche Datenschutzaufsichtsbehörden im europäischen Verbund zuschreiben, (2) föderale Fragmentierung mit 18 Behörden auf Bundes- und Landesebene, (3) erhebliche Ausstattungsunterschiede, die einzelnen Länderbehörden mit weniger als 15 Mitarbeitenden eine effektive Aufgabenerfüllung einschließlich innovationsbegleitender Beratungsmaßnahmen faktisch (sehr) schwierig machen.[20]

---

[15] *Draghi*, The Future of European Competitiveness, 2024, Part A, ch. 2, p. 30
[16] *Draghi*, The Future of European Competitiveness, 2024, Part B, sec. 2, ch. 5, p. 319.
[17] *Draghi*, The Future of European Competitiveness, 2024, Part A, ch. 1, p. 18.
[18] *Draghi*, The Future of European Competitiveness, 2024, Part B, sec. 2, ch. 5, p. 319.
[19] *Draghi*, The Future of European Competitiveness, 2024, Part B, sec. 2, ch. 5, p. 322, 326, statt vieler.
[20] wida, Strategische Überlegungen zur Zukunft der europäischen Datenschutzaufsicht – unter besonderer Berücksichtigung der Aufsicht in Deutschland, 2025, 14 ff. abrufbar unter: https://wida.digital/assets/images/Strategie_DS_EU_GV_6-25.pdf.

Die vom Draghi-Report beschriebenen Defizite – i.e. Rechtsunsicherheit, Compliance-Last und innovationsfeindliche Risikokultur – sind für Unternehmen in der täglichen Praxis unmittelbar erfahrbar. Der Befund des Berichts wird durch aktuelle empirische Erhebungen nicht nur bestätigt, sondern in seinem Ausmaß sogar noch verstärkt. So hat die dänische Regierung in ihrer Stellungnahme zum Digital Omnibus vom 14. Oktober 2025 festgehalten, dass die DSGVO-Compliance dänische Unternehmen – einschließlich nationaler Folgegesetzgebung – rund 2 Mrd. EUR jährlich kostet. Viele Initiativen im privaten und öffentlichen Sektor werden demnach wegen DSGVO-Compliance-Unsicherheiten pausiert oder aufgegeben; kleine Unternehmen und gemeinnützige Organisationen tragen die hierdurch induzierte Last überproportional. Die dänische Regierung spricht sich daher explizit für einen stärker risikobasierten Ansatz aus, „bei dem regulatorische Anforderungen proportional zu den tatsächlich mit der Datenverarbeitung verbundenen Risiken sind."[21] In diesem Sinne hat die deutsche Bundesregierung in ihrem Vorschlag zur Vereinfachung der DSGVO vom 23. Oktober 2025 nach Konsultation relevanter Stakeholder festgestellt, dass die Omnibus-Vorschläge „nicht weit genug gehen" – und ein zweistufiges Reformmodell (kurzfristige Omnibus-Maßnahmen plus tiefgreifendere Änderungen im Digital Fitness Check) vorgelegt, das mit dem in diesem Impulspapier entwickelten Ansatz konvergiert.[22]

Die vorstehend erhobenen Befunde werden durch ökonometrische Forschungsergebnisse gestützt, wonach das US-amerikanische Risikokapitalengagement in Europa nach Inkrafttreten der DSGVO um mehr als 20 % zurückgegangen ist.[23] Dass sich regulatorische Unsicherheit nicht nur in Investitionsentscheidungen, sondern darüber hinaus auch in konkreten Produktverzögerungen und beschränkten Funktionsumfängen niederschlägt, bestätigen Unternehmen in ihren Stellungnahmen zum Digital Fitness Check.[24] Europas Anteil an der globalen Marktkapitalisierung im Bereich Technologie, Medien und Telekommunikation (TMT) ist von 30 % (2000) auf 7 % (2024) gefallen.[25] Die USA

---

[21] "Specifically, Denmark encourages an even more risk-based approach, where regulatory requirements are proportionate to the actual risks involved in data processing." Ministry of digital affairs, The Danish Government's response to the Commission's call for evidence for the Digital Omnibus as regards the digital area, S. 4, online abrufbar: https://www.ft.dk/samling/20251/almdel/DIU/bilag/5/3081852.pdf.

[22] German proposal for simplification of the GDPR, online abrufbar: https://cdn.netzpolitik.org/wp-upload/2025/11/German-Proposal-for-simplification-of-the-GDPR.pdf.

[23] *Jia/Jin/Leccese/Wagman*, How Does Privacy Regulation Affect Transatlantic Venture Investment? Evidence from GDPR, NBER Working Paper No. 33909 (Juni 2025).

[24] Vgl. auch Stanford HAI, AI Index Report 2025 (40 bedeutende KI-Modelle in den USA, 15 in China, 3 in der gesamten EU im Jahr 2024).

[25] *Sehdev/Vanderspar* et. al., Technology, media, and telecom in Europe: The new growth engine or another decade of missing out?, 21.05.2025, online abrufbar: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-

haben 2024 rund 109 Mrd. USD in KI investiert; demgegenüber liegt Europa nur bei einem Bruchteil dieses Betrags.[26] Europa verfügt über schätzungsweise 5 % der globalen KI-Rechenkapazität gegenüber 74 % in den USA.[27] Der Draghi-Report identifiziert einen jährlichen Investitionsrückstand von 800 Mrd. EUR, für den die Datenregulierung als materieller Hemmfaktor benannt wird.[28] Dänische Unternehmen tragen – wie vorstehend ausgeführt – allein durch DSGVO-Compliance jährliche Kosten von rund 2 Mrd. EUR; für den Wirtschaftsstandort München-Oberbayern mit seinem überdurchschnittlichen Anteil datenintensiver Branchen (i.e. Automotive, Medizintechnik, Finanzdienstleistungen, Plattformwirtschaft) sind vergleichbare Kosten anzunehmen. Diese Zahlen belegen, dass das vorliegende Reformprogramm keine rechtspolitische Kür, sondern eine strategische Notwendigkeit für die Wettbewerbsfähigkeit Europas und Deutschlands darstellt.

Die fehlende Realisierung der Potenziale und Schlagkraft des Digitalen Binnenmarkts bildet ein substanzielles strukturelles Hindernis für die europäische Wettbewerbsfähigkeit. Innovation und Regulierung, hier konkret der Datenökonomie, sind keine natürlichen Gegensätze, sondern Regulierung kann durch die Herstellung von Rechtssicherheit und der Ermöglichung von belastbaren Planungen die Innovationskraft gerade auch stärken. Die Reformimpulse des vorliegenden Impulspapiers sind insofern nicht als Abschwächung des Datenschutzes zu verstehen, sondern vielmehr als eine Rückbesinnung auf eine pluralistische (Grund-)Rechtsordnung, die auf den verhältnismäßigen Ausgleich von Interessen und Rechtspositionen bei Kollisionslagen setzt.

IV. Zusammenspiel der europäischen Digital- und Datenrechtsakte

Weitere substanzielle Hemmnisse für die Innovation ergeben sich auch und gerade aus dem Zusammenspiel der europäischen Digital- und Datenrechtsakte. Insoweit ist insbesondere das Verhältnis zwischen dem DA und der DSGVO hervorzuheben. Aufgrund (scheinbar) gegensätzlicher Stoßrichtungen zwischen dem Teilen von Daten und der zurückhaltenden Verarbeitung personenbezogener Daten besteht ein Spannungsverhältnis.[29] Denn die DSGVO mahnt durch Grundsätze wie „Privacy by

---

insights/technology-media-and-telecom-in-europe-the-new-growth-engine-or-another-decade-of-missing-out.

[26] Statista, Private Investitionen im Bereich Künstliche Intelligenz (KI) nach Region in den Jahren 2013 bis 2024, online abrufbar: https://de.statista.com/statistik/daten/studie/1321969/umfrage/private-investitionen-in-ki-nach-region/.

[27] *Steinschaden*, „Europa konsumiert KI intensiv, stärkt dabei aber primär fremde Ökosysteme“, 16.03.2026, online abrufbar: https://www.trendingtopics.eu/ai-research-2026-europe-vs-usa-vs-china/.

[28] *Draghi*, The Future of European Competitiveness, 2024, Part A, ch. 5, p. 63.

[29] *Paal*, GRUR 2026, 361, 369.

Design“ und „Privacy by Default“ (Art. 25 Abs. 1, 2 DSGVO) zur zurückhaltenden Datenverarbeitung, der DA verlangt demgegenüber einen umfangreichen Datenzugriff („Access by Design“, vgl. Art. 3 Abs. 1 DA: „Vernetzte Produkte werden so konzipiert […]“). Verantwortliche sind vor diesem Hintergrund vielfach auf einen Drahtseilakt zwischen einem Verstoß gegen einerseits die DSGVO oder andererseits den DA verwiesen, während beide Rechtsakte kumulativ neue (Informations-)Pflichten vorsehen. Die Regelungsregime selbst tragen unmittelbar wenig zur Auflösung dieser Spannungslage und der hieraus entstehenden innovationshemmenden Belastungen bei. Art. 1 Abs. 5 DA spricht von einer „unbeschadet[en]“ Geltung der DSGVO, wobei im Fall von Kollisionen die DSGVO Vorrang haben soll.

Besonders deutlich zeigt sich dieses Spannungsverhältnis in ErwGr. 7 S. 7 DA. Hiernach stellt der DA „keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber dar“. Die Notwendigkeit einer Rechtsgrundlage unter der DSGVO für allfällige Verarbeitungen von personenbezogenen Daten unter dem DA unterstreichen zugleich sowohl Art. 4 Abs. 12 DA als auch Art. 5 Abs. 7 DA. Vor allem wenn der Zugang zu solchen Datenkategorien betroffen ist, die auch personenbezogene Daten Dritter enthalten, stellen sich Fragen der Datenschutzrechtskonformität und nach einer eventuellen Vereitelung von Datenzugangsansprüchen durch das Datenschutzrecht. Denn als datenschutzrechtliche Rechtsgrundlage kommt grundsätzlich nur Art. 6 Abs. 1 lit. f) DSGVO in Betracht, der jedoch aufgrund der Einzelfallabhängigkeit der erforderlichen Interessenabwägung in der Praxis mit weitreichenden Unsicherheiten verbunden ist.[30] Der Dateninhaber steht somit vor einem Dilemma: Verweigert der Dateninhaber den Anspruch nach dem DA aufgrund von datenschutzrechtlichen Bedenken, könnte er bei einer Fehleinschätzung nach dem Sanktionsregime des DA haften. Erfüllt der Dateninhaber den DA-Anspruch, kann bei einer datenschutzrechtlichen Fehleinschätzung das Sanktionsregime der DSGVO zur Anwendung berufen sein.[31]

Diese Rechtsunsicherheit gepaart mit einer kumulativen Belastung aus sich überschneidenden Pflichtenregimen beeinträchtigt erheblich das Innovationspotenzial des Digitalen Binnenmarkts.

V. Notwendigkeit eines Paradigmenwechsels

In Ansehung der vielfach monofokussierten Anwendung und Auslegung der DSGVO-Vorgaben auf den Datenschutz unter Vernachlässigung anderer elementarer

---

[30] *Paal*, GRUR 2026, 361, 369 f. m.w.N.
[31] Vgl. *Paal*, GRUR 2026, 361, 370.

Grundrechte und -freiheiten sowie Interessen bleibt die Nutzung von Daten gegenwärtig deutlich hinter den Potenzialen für Innovation zurück.[32] In Verbindung mit der Verwendung eines faktischen Null-Risiko-Ansatzes durch zahlreiche Aufsichtsbehörden und Gerichte, so u.a. bei Fragen der Rechtfertigung von Datenverarbeitungen, bei Betroffenenrechten, Interessenabwägungen und beim internationalen Datentransfer, fehlt es an einem angemessenen, verhältnismäßigen Ausgleich von Datenschutz und anderen Grundrechten im Kollisionsfall.

So bleibt bislang das, prominent bereits in Art. 1 DSGVO verankerte, zweite DSGVO-Hauptziel systematisch unterbelichtet, nämlich die Förderung des freien Datenverkehrs. Zugleich wird der strukturell und systematisch gleichberechtigte Schutz natürlicher Personen bei der Datenverarbeitung durch die Aufsichtsbehörden in ihrer Auslegungspraxis faktisch zum tragenden Grundprinzip heraufgestuft. Die Harmonisierung des Datenschutzniveaus soll auch und gerade den freien Datenverkehr fördern. Die zweite DSGVO-Zielsetzung in Gestalt des freien Datenverkehrs stützt einen proaktiven Umgang mit der Datennutzung. Dies gilt vor allem auch im Lichte zahlreicher jüngerer EU-Digitalrechtsakte (z. B. DA, DGA, EHDS-VO, KI-VO), die eine solche Datennutzung faktisch voraussetzen.

Für die DSGVO erfolgt in der gegenwärtigen Anwendungs- und Auslegungspraxis überdies vielfach ein One-size-fits-all-Ansatz, der sämtliche Datenverarbeitungen – unabhängig von dem konkreten Risiko, dem Kontext oder der konkreten Rolle und Stellung der beteiligten Akteure – mit ähnlicher Intensität adressiert und reguliert. Dies führt zu einer systematischen Überlastung insbesondere in jenen Bereichen, in denen geringe(re) Risiken bei zugleich hohem Innovationspotenzial bestehen. Der Grundgedanke eines abgestuften, differenzierten und risikobasierten Regelungsregimes unter komplementärer Förderung von Datenschutz und -Nutzung tritt dabei in den Hintergrund.

Dass dieser Befund keine bloße rechtspolitische Kritik darstellt, sondern im laufenden Gesetzgebungsverfahren unmittelbare praktische Relevanz entfaltet, zeigt die gemeinsame Stellungnahme des Europäischen Datenschutzausschusses (EDSA) und des Europäischen Datenschutzbeauftragten (EDSB) (Joint Opinion 2/2026 vom 10. Februar 2026) zu den Digital Omnibus-Vorschlägen:[33] In beiden für die vorliegende Untersuchung besonders relevanten Punkten – der Definition des Personenbezugs und der Rechtsgrundlage für das KI-Training – haben der EDSA/EDSB die

---

[32] Vgl. statt vieler *Specht-Riemenschneider*, ZEuP 2023, 638, 641.

[33] Online abrufbar: https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf.

Kommissionsvorschläge abgelehnt oder unter erheblichen Vorbehalt gestellt. Dies unterstreicht, dass eine normative Reform allein nicht ausreicht; ohne eine Änderung der Auslegungspraxis und der institutionellen Anreizstruktur drohen legislative Fortschritte an der Aufsichtspraxis zu scheitern.

Mit Blick auf das Gesamtbild dieser (Fehl-)Entwicklungen empfiehlt sich daher ein Paradigmenwechsel im rechtlichen und regulatorischen Umgang mit Daten. Hierdurch können Harmonisierung, Rechtssicherheit und Innovationsoffenheit bei Datenschutz und Datennutzung ermöglicht werden, die im Einklang mit den übergreifenden politischen Zielen stehen. Zugleich gilt es zu verhindern, dass selbst risikoarme und gesamtgesellschaftlich wünschenswerte Datenverarbeitungen durch eine überschießende Auslegung der DSGVO-Vorgaben blockiert werden.

B. Grundrechtsdogmatische Ausgangslage: Datenschutz als abwägungsfähiges Grundrecht

Mit dem vorgeschlagenen Paradigmenwechsel soll keinesfalls ein Rückbau des Datenschutzniveaus zugunsten einer unbegrenzten Datennutzung erreicht werden. Vielmehr geht es um die erforderliche Neujustierung eines angemessenen Ausgleichs zwischen den betroffenen Grundrechten, Grundfreiheiten und Interessen. Das übergeordnete Ziel des vorgeschlagenen Ansatzes ist die Förderung einer differenzierten, grundrechtsschützenden und innovationsfreundlichen Auslegung und Anwendung des Datenschutzrechts als eines zentralen Bestandteils des sich entwickelnden Daten(nutzungs)rechts.

I. Art. 7, 8 GRCh: keine „Super“-Grundrechte

Das Recht auf Schutz personenbezogener Daten ist durch Art. 8 GRCh als eigenständiges EU-Grundrecht gewährleistet. Art. 8 GRCh tritt neben das Recht auf Achtung des Privat- und Familienlebens nach Art. 7 GRCh und bildet die primärrechtliche Grundlage der DSGVO. In einer langen Reihe von Entscheidungen hat der EuGH belastbar herausgearbeitet, dass Art. 8 GRCh gerade kein absolutes Recht gewährt.[34] Richtigerweise muss das Grundrecht auf Datenschutz im Lichte seiner gesellschaftlichen Funktion betrachtet und nach Maßgabe des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.[35]

---

[34] EuGH, Urt. v. 26.07.2017 – Gutachten 1/15, BeckRS 2017, 123252, Rn. 136; EuGH, Urt. v. 17.10.2013 – C-291/12, Schwarz, BeckRS 2013, 81987, Rn. 33; EuGH, Urt. v. 05.05.2011 – C-543/09, Deutsche Telekom, EuZW 2011, 484, 487, Rn. 51; EuGH, Urt. v. 09.11.2010 – C-92, 93/09, Volker und Markus Schecke, EuZW 2010, 939, 941, Rn. 48; EuGH, Urt. v. 12.06.2003 – C-112/00, Schmidtberger, NJW 2003, 3185, 3188, Rn. 80, welches sich aber nicht auf Art. 8 GRCh bezieht.
[35] *Paal*, ZfDR 2026, 1, 11; *Wünschelbaum*, NJW 2026, 950, 951.

Diese Aussage ist normativ in Art. 52 Abs. 1 GRCh verankert: Einschränkungen der in der Charta anerkannten Rechte müssen gesetzlich vorgesehen sein, den Wesensgehalt achten, dem Verhältnismäßigkeitsgrundsatz genügen und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen tatsächlich entsprechen. Für KI-bezogene Datenverarbeitungen hat dieser Befund erhebliche praktische Konsequenzen: Mit der unternehmerischen Freiheit nach Art. 16 GRCh, der Eigentumsgarantie nach Art. 17 GRCh und dem Recht auf Informationsfreiheit nach Art. 11 GRCh stehen dem Datenschutz gewichtige Grundrechte gegenüber, die bei der Auslegung der DSGVO zwingend in die Abwägung einzubeziehen sind.[36]

Unter Rekurs auf Art. 54 GRCh, der die absolutistische Ausnutzung eines Rechts zum Nachteil anderer Grundrechte verbietet, ist eine stärkere Verhältnismäßigkeitsorientierung der DSGVO-Anwendungspraxis anzumahnen. Ausgangspunkt für das Zusammenspiel des Datenschutzes mit anderen Grundrechten und Grundfreiheiten im Hinblick auf eine Verbesserung und Förderung von Datennutzung bildet die Feststellung, dass das Datenschutzgrundrecht aus Art. 7 und 8 GRCh gerade kein schrankenlos gewährtes (Super-)Grundrecht verkörpert. Vielmehr muss der Datenschutz stets (auch) im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Grundsatzes der Verhältnismäßigkeit mit gegebenenfalls kollidierenden anderen Grundrechten abgewogen werden.

II. Abwägungspflicht nach ErwGr. 4 DSGVO und die doppelte Zielsetzung des Art. 1 DSGVO

In ErwGr. 4 S. 2 DSGVO ist ausdrücklich niedergelegt, dass das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht darstellt; „es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.“ Zur Herstellung eines zutreffend ausbalancierten Datenschutzverständnisses sollte ErwGr. 4 DSGVO, der die Abwägung mit anderen Grundrechten und die gesellschaftliche Funktion des Datenschutzes betont, systematisch gegenüber ErwGr. 10 DSGVO (betreffend ein gleichwertiges Datenschutzniveau) stärker berücksichtigt werden, um einen verhältnismäßigen, kontextsensiblen Regulierungs- und Durchsetzungsansatz zu erreichen. Denn ErwGr. 10 DSGVO, der das Ziel eines „einheitlichen und hohen Schutzniveaus“ benennt, wird bislang vielfach (zu Unrecht) faktisch als ein Maximierungsgebot interpretiert. Die hieraus erwachsende Verabsolutierung des Schutzzwecks verkennt das unionsrechtliche Gebot der

[36] So auch *Wünschelbaum*, NJW 2026, 950, 951.

Verhältnismäßigkeit (Art. 52 Abs. 1 GRCh) und begünstigt eine gesetzgeberisch gerade nicht intendierte, innovationshemmende Überregulierung.[37]

Weiterhin ist erneut hervorzuheben, dass Art. 1 DSGVO eine duale Zielsetzung verfolgt, nämlich zum einen den Schutz personenbezogener Daten (Abs. 1 und 2) und zum anderen komplementär die Sicherung des freien Verkehrs personenbezogener Daten (Abs. 1 und 3). Die zweite Zielsetzung – sprich der freie Datenfluss – ist in der Auslegungspraxis bislang systematisch unzureichend berücksichtigt worden.

Die Abwägungspflicht ist nicht lediglich eine deklaratorische Auslegungshilfe. Vielmehr ist die Abwägungspflicht ein Ausdruck der zwingenden grundrechtlichen Wertungsordnung der GRCh und damit unmittelbar verbindlich für alle Organe der Union und der Mitgliedstaaten, die das Unionsrecht durchführen (Art. 51 Abs. 1 GRCh).[38] Datenschutzaufsichtsbehörden als Behörden, die das Unionsrecht – so auch und gerade die DSGVO – durchführen, sind daran gebunden.

Zu erwägen ist deshalb ein gezielter legislativer Impuls zur Stärkung der Abwägungspflicht durch Ergänzung von ErwGr. 4 DSGVO, um eine explizite Bezugnahme auf die Pflicht der Datenschutzaufsichtsbehörden, Folgenabschätzungen zur Bewertung der Verhältnismäßigkeit und der Auswirkungen des Datenschutzes auf andere Rechte, wesentliche öffentliche Interessen und nachhaltige Innovation durchzuführen.

Die Arbeitsgruppe DSGVO am TUM Think Tank hat in diesem Sinne einen konkreten Vorschlag zur Anpassung von ErwGr. 4 im Lichte des risikobasierten Ansatzes[39] entwickelt:

„Gemäß Absatz 3 von Artikel 5 sind die allgemeinen Datenschutzgrundsätze und die übrigen Vorgaben dieser Verordnung so auszulegen, dass sie in einem angemessenen Verhältnis zu dem mit den jeweiligen Vorgaben dieser Verordnung verfolgten Zweck stehen und dass sie den freien Verkehr personenbezogener Daten nicht unangemessen beeinträchtigen.

Das Recht auf Schutz personenbezogener Daten und die Interessen oder Grundrechte und Grundfreiheiten anderer Personen als der betroffenen Person sind von den

---

[37] Vgl. auch *Paal*, ZfDR 2026, 1, 10.
[38] Statt vieler allgemein von der Groeben/Schwarze/Hatje/Terhechte/*Breitenmoser/Weyeneth*, 8. Aufl. 2025, Art. 67 AEUV Rn. 33.
[39] Zum risikobasierten Ansatz sogleich unter C.

Verantwortlichen, den Aufsichtsbehörden und Gerichten in einen angemessenen Ausgleich zu bringen.

Damit soll sichergestellt werden, dass sich auch das zweite in Absatz 1 von Artikel 1 genannte Ziel dieser Verordnung in den Datenschutzgrundsätzen nach Artikel 5 wiederfindet und dass die in Erwägungsgrund 4 genannte Abwägung zwischen dem Recht auf Schutz der personenbezogenen Daten und anderen Grundrechten stattfinden kann.

Zu den Grundrechten und geschützten Interessen, die mit dem Recht auf Schutz personenbezogener Daten gegebenenfalls in einem Spannungsverhältnis stehen, gehören insbesondere Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, und Vielfalt der Kulturen, Religionen und Sprachen sowie die Wissenschafts- und Forschungsfreiheit. Aber auch das Recht auf Achtung des Privat- und Familienlebens sowie das Recht auf Datenschutz Dritter sind zu berücksichtigen, etwa wenn die durch eine betroffene Person gegebene Einwilligung in die Verarbeitung ihrer personenbezogenen Daten auch Auswirkungen auf andere Personen hat, deren personenbezogene Daten nicht unmittelbar verarbeitet wurden, die aber persönliche Merkmale mit der betroffenen Person, deren Daten verarbeitet wurden, teilen.

Besondere Bedeutung kommt in diesem Zusammenhang dem risikobasierten Ansatz zu, welcher auch andere Rechtsakte der Union, namentlich Verordnungen (EU) 2022/2065 und (EU) 2024/1689 prägt. Nach diesem risikobasierten Ansatz haben durch Regulierung begründete Rechte und Pflichten, die zum Schutz gegen die Verwirklichung von Risiken für Sicherheit, Gesundheit und andere Grundrechte geschaffen wurden, stets in einem angemessenen Verhältnis zur Schwere dieser Risiken zu stehen. Der Begriff des Risikos soll dabei im Einklang mit anderen Vorschriften dieser Verordnung und ihren Erwägungsgründen, namentlich Erwägungsgründen 75 ff., verstanden werden und unter anderem Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person vor dem Hintergrund von Art, Umfang, Umständen und Zwecken der Verarbeitung berücksichtigen. Dabei sollte auch der Anzahl der von seinen Verarbeitungstätigkeiten betroffenen Personen, wesentliche Bedeutung zukommen."[40]

[40] Abrufbar unter: https://tumthinktank.de/wp-content/uploads/DSGVO_RisikobasierterAnsatz_V1.pdf.

Ergänzend könnte in Art. 51 DSGVO ausdrücklich normiert werden, dass Aufsichtsbehörden die Ausgewogenheit und Verhältnismäßigkeit gemäß ErwGr. 4 DSGVO und den Art. 52, 54 GRCh in ihrer Abwägung zu gewährleisten haben.

III. Null-Risiko-Ansatz bei der DSGVO-Interpretation ist abzulehnen

In der Aufsichtspraxis einer nicht unerheblichen Zahl europäischer Datenschutzaufsichtsbehörden ist eine Auslegungstradition entstanden, die den Datenschutz faktisch als schrankenlos zu gewährleistende Maximalposition behandelt.[41] Personenbezogene Daten werden hierbei als per se gefahrgeneigt qualifiziert, ihre Minimierung gilt als oberstes Optimierungsziel unabhängig von Umfang oder Schwere der tatsächlichen Risiken für betroffene Personen. Auf KI-bezogene Datenverarbeitungen wird dieser Ansatz besonders restriktiv angewendet.[42]

Dieser Null-Risiko-Ansatz folgt nicht zuletzt aus der grundsätzlichen Problematik im Zusammenhang mit den durch das Datenschutzrecht zu schützenden Rechtsgütern. Anders als in anderen Rechtsordnungen, in denen datenschutzrechtliche Instrumente klar an abgrenzbare grundrechtliche Positionen wie die Privatsphäre (etwa die US-amerikanischen Ansätze des Privacy-Schutzes) oder den Persönlichkeitsschutz (wie der Ansatz im schweizerischen DSG, der strukturell am Konzept der Persönlichkeitsverletzung aufgebaut ist[43]) anknüpfen, ist der in der europäischen (und deutschen) Tradition stehende Datenschutz hiervon zunächst entkoppelt. Strukturelle Konsequenz hiervon ist, dass jede Datenverarbeitung im Ausgangspunkt gleichbehandelt wird, wie etwa durch das die DSGVO prägende generelle Verbot mit Erlaubnisverbot, welches für alle Verarbeitungen personenbezogener Daten einen „one size fits all"-Ansatz vorsieht. Der hieraus abgeleitete generelle Schutzbedarf macht es schwierig, den Datenschutz als das zu verstehen, was er in einem risikobasierten Konzept sein sollte: ein Katalog von Instrumenten, der schützenswerte Grundrechtspositionen natürlicher Personen im Blick hat und entsprechend ihres Gewichts im Einzelfall ausgleicht.

Der Null-Risiko-Ansatz ist rechtsdogmatisch abzulehnen, da er die Abwägungspflicht aus Art. 8, 52 Abs. 1 GRCh und ErwGr. 4 DSGVO verletzt. Zudem kollidiert der Null-Risiko-Ansatz mit dem in Art. 1 Abs. 3 DSGVO verankerten Ziel des freien Datenverkehrs und missachtet den der DSGVO zugrundeliegenden risikobasierten Ansatz, der unter anderem in Art. 24, 25, 32 und 35 DSGVO normativ verankert ist.

---

[41] *Christakis*, The Zero Risk Fallacy, 2024, S. 15 ff.; *Paal*, NJW 2024, 3681, 3682 f., Rn. 8 ff., m.w.N.
[42] Ähnlich *Draghi*, The Future of European Competitiveness, 2024, Part A, ch. 2, p. 30.
[43] S. insbesondere Art. 30 f. DSG (Schweiz).

Pointiert lässt sich dieser Befund dahingehend zusammenfassen, dass gerade die vermeintlich perfekte, absolutistische Durchsetzung der DSGVO in ihr Gegenteil umzuschlagen droht: Eine bis zur Schrankenlosigkeit getriebene Schutzmaximierung erzeugt nicht mehr, sondern weniger Grundrechtsverwirklichung, weil sie kollidierende Rechte und Freiheiten verdrängt und gravierende Rechtsunsicherheiten hervorruft. Die kritische Auseinandersetzung mit der Anwendung und Auslegung der DSGVO sowie der einschlägigen Aufsichtspraxis ist daher nicht als Geringschätzung des Datenschutzes, sondern vielmehr als notwendige Korrektur zur Herstellung von Verhältnismäßigkeit und praktischer Konkordanz zu verstehen.

Wird das KI-Training pauschal als datenschutzwidrig qualifiziert, ohne die tatsächliche Risikosituation zu prüfen, ist dies weder in Übereinstimmung mit dem Gesetzeswortlaut noch mit dem Telos des geltenden Rechts. Vielmehr droht eine in diesem Sinne verabsolutierte Rechtsanwendung – bei der das sekundärrechtliche Instrument der DSGVO faktisch die Wirkung von Primärrecht mit Verfassungsrang entfaltet – in Widerspruch mit dem Unionsrecht zu geraten. Dieser Konflikt ist zudem die Konsequenz einer auf Grundrechteebene (insbes. Art. 8 GRCh) fehlenden positiven Konzeptualisierung eines sachlichen Schutzbereichs. Denn der „Schutz personenbezogener Daten“ kann von Gerichten oft gerade nur durch Heranziehung des Sekundärrechts verstanden werden, zumal die Grundrechtsqualifizierung des Datenschutzes der historischen Entwicklung des (einfachen) Datenschutzrechts zeitlich nachgelagert war. In dieser Hinsicht sollte eine Rückbesinnung auf die ursprünglich das Datenschutzrecht inhaltlich begründende Grundrechtspositionen erfolgen, wie sie etwa dem Volkszählungs-Urteil des BVerfG[44] zugrunde liegen. So kommt auch der EGMR mit dem Grundrecht auf Achtung des Privatlebens (Art. 8 EMRK) zurecht,[45] um datenschutzrechtlich relevante Sachverhalte angemessen zu lösen. Ein verstärkter Fokus auf die Abwägung von Privatheit gegen andere Grundrechte, wofür das Datenschutzrecht ein Werkzeug, nicht jedoch das Ziel, ist, wäre in vielen Konstellationen als Maßstab tauglicher – und für Gerichte handhabbarer. Ein solcher Ansatz kann auf dem bestehenden Art. 6 Abs. 1 lit. f) DSGVO aufbauen[46] und diesen Rechtfertigungstatbestand als Ausgangspunkt für eine weitergehende Interessenabwägung heranziehen.

---

[44] BVerfG, Urt. v. 13.04.1983 – 1 BvR 209/83, 1 BvR 269/83, NJW 1983, 1307.
[45] Beispielhaft EGMR, Urt. v. 28.06.2018 – Nr. 60798/10 und 65599/10, M.L. und W.W. gegen Deutschland; grundlegend zu Art. 8 GRCh EGMR, Urt. v. 07.02.2012 – Nr. 40660/08 und 60641/08, von Hannover gegen Deutschland (Nr. 2), NJW 2012, 1053.
[46] Hierzu sogleich unter C. IV. 1.

IV. Innovation als Grundrechtsdimension

Es kann mit guten Gründen argumentiert werden, dass ein zukunftsfähiger Ordnungsrahmen die positiven Entfaltungsmöglichkeiten digitaler Technologien aktiv ermöglichen sollte, um zur Grundrechtsverwirklichung beizutragen.[47] Dies betrifft insbesondere den Umgang mit personenbezogenen Daten als eine der zentralen Voraussetzungen für datengetriebene Innovation. Denn eine einseitige Aktivierung der Datenschutzvorgaben droht individuelle und gesellschaftliche Chancen zu blockieren.

Dieser Befund betrifft auch und gerade Konstellationen, in denen durch eine weitgehende Anonymisierung und technische Schutzmaßnahmen ein nur geringes Risiko für den Schutz personenbezogener Daten besteht. Der Schutz personenbezogener Daten sollte nicht losgelöst von den digitalen Rechten und Möglichkeiten gedacht werden, die durch KI gerade erst realisiert oder verbessert werden können – wie etwa Rechte betreffend Gesundheit, Bildung, Mobilität oder Teilhabe. Vor diesem Hintergrund kann der Staat nicht nur zum Schutz, sondern auch zur aktiven Ermöglichung digitaler Teilhabe verpflichtet sein – konkret durch den angemessenen Ausgleich strukturell gleichrangiger (Grund-)Rechtspositionen und Interessen, mit der Folge fairer Datenzugänge und innovationsfreundlicher Auslegung(en) bestehender Normen.[48]

Innovation ist nicht lediglich ein wirtschaftspolitisches Interesse, sondern kann sich als eine Dimension der Grundrechteentfaltung darstellen (z.B. mit Blick auf Art. 16 GRCh), indem neuen Herausforderungen begegnet und die Verwirklichung dieser Rechte in der Praxis erweitert werden kann.[49] Dieser Befund ist nicht primär als rechtspolitisches Postulat zu verstehen, sondern als Ausdruck der geltenden Grundrechtsdogmatik: Art. 52 und 54 GRCh gebieten die Einbettung jedes Rechts aus der Charta – also auch des Datenschutzgrundrechts aus Art. 8 GRCh – in eine pluralistische Grundrechtsordnung, die keinem einzelnen Recht einen Absolutheitsrang einräumt. Der Vorschlag, in den DSGVO-Erwägungsgründen sowie in Art. 5 DSGVO ausdrücklich die notwendige Balance zwischen Datenschutz und Innovation als

---

[47] *Guzzetta*, Le sfide dell'intelligenza artificiale. Il diritto di fronte all'innovazione e l'innovazione come diritto, 2025, https://www.fondazioneluigieinaudi.it/wp-content/uploads/2025/01/rapporto-guzzetta-ia-diritto-innovazione-30012025.pdf.

[48] *Paal*, ZfDR 2026, 1, 32.

[49] *„Innovation is essential for safeguarding and advancing fundamental rights, including privacy. It empowers us to address emerging challenges and to expand how these rights are manifested in practice. For innovation and progress to be truly sustainable, fundamental rights must be carefully considered and balanced, ensuring that new solutions benefit all individuals by respecting and advancing their diverse rights and interests."* – Instituto Italiano per la Privacy e la Valorizzazione dei Dati, Proposals for Improving the Digital Omnibus, Rebalancing Data Protection and E-Privacy Disciplines with Innovation, Positioning Paper, Rom, Februar 2026, S. 4

Ausdruck anderer Rechte und Freiheiten zu verankern, stellt sich daher nicht als Absenkung des Datenschutzniveaus dar, sondern als seine normativ gebotene Rückführung in die vorgefundene pluralistische Grundrechtsordnung.

V. Verankerung eines Innovationsmandats

Art. 1 DSGVO enthält *de lege lata* keinen expliziten Verweis auf Innovation oder wirtschaftliche Entwicklung als Regelungsziele. Diese normative Lücke ist für den KI-Kontext besonders nachteilig, denn Behörden und Gerichte mögen vor diesem Hintergrund zu einer einseitig schutzorientierten Auslegung der DSGVO kommen.

Vor diesem Hintergrund empfiehlt sich die Aufnahme eines Art. 1 Abs. 3a DSGVO in den Normtext, um Innovation, digitale Entwicklung und die Wettbewerbsfähigkeit der Union als gleichrangige Ziele neben dem Datenschutz zu verankern:

„(3a) Diese Verordnung wird angewendet, um zugleich Innovation, digitale Entwicklung und die Wettbewerbsfähigkeit der Union neben dem Schutz personenbezogener Daten im Einklang mit dem Unionsrecht zu fördern. Die Aufsichtsbehörden haben bei der Wahrnehmung ihrer Aufgaben die Wechselwirkungen zwischen Datenschutz, gesamtgesellschaftlichem Nutzen, technologischem Fortschritt und wirtschaftlicher Entwicklung zu berücksichtigen.“

Ergänzend sollte die Formulierung in ErwGr. 10 DSGVO von einem „hohen“ auf ein „angemessenes“ Schutzniveau umgestellt werden. Denn die bisherige Formulierung wird (auch und gerade) vom EuGH als faktischer Maximierungsstandard interpretiert,[50] was mit dem unionsrechtlichen Verhältnismäßigkeitsgebot des Art. 52 Abs. 1 GRCh kaum in Einklang zu bringen ist.[51]

Das Innovationsmandat für Datenschutzaufsichtsbehörden ist zudem primärrechtlich abgesichert: Art. 3 EUV verpflichtet die Union auf nachhaltige wirtschaftliche Entwicklung und Wettbewerbsfähigkeit; Art. 16 GRCh schützt die unternehmerische Freiheit als Grundrecht. Vor diesem verfassungsrechtlichen Hintergrund ist das Innovationsmandat eine Konkretisierung bereits bestehender primärrechtlicher Verpflichtungen. Dem Art. 1 Abs. 3a DSGVO-E (Innovationsmandat) und der *de lege ferenda* in Art. 51 DSGVO zu verankernden Innovationspflicht für Aufsichtsbehörden fehlt jedoch ein Rechenschaftsmechanismus, der die Pflicht nach außen sichtbar und nachprüfbar macht. Dieser Mechanismus könnte durch eine Ergänzung des Art. 57 DSGVO etabliert werden: Aufsichtsbehörden sollten in ihren Tätigkeitsberichten

[50] *Paal*, ZfDR 2026, 1, 10.
[51] *Paal*, ZfDR 2026, 1, 10.

verpflichtend darlegen, wie ihre Leitlinienpraxis und Vollzugsentscheidungen zu Rechtssicherheit, ausgewogener Aufsicht und den Innovations- und Wettbewerbszielen der Union beigetragen haben.

Der Digital Omnibus greift diese Reformrichtung jedenfalls punktuell auf. Die EU-Kommission schlägt insoweit die Klarstellung vor, dass die Verarbeitung personenbezogener Daten für KI-Training auf Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse) gestützt werden kann. Dies ist ein wichtiger erster Schritt in die richtige Richtung, löst aber das strukturelle Problem (noch) nicht zufriedenstellend. Denn eine Klarstellung auf Ebene einzelner Erlaubnistatbestände ohne gleichzeitige normative Verankerung eines Innovationsmandats in Art. 1 DSGVO bleibt fragmentarisch. Datenschutzaufsichtsbehörden, die eine schutzmaximierende Auslegungstradition verfolgen, könnten die Klarstellung zu Art. 6 DSGVO in der Praxis weitgehend leerlaufen lassen, solange Art. 1 DSGVO keine gleichrangige explizite Innovationszielsetzung enthält. Der vorgeschlagene Art. 1 Abs. 3a DSGVO versteht sich damit nicht als eine Alternative zum Digital Omnibus-Vorschlag, sondern vielmehr als dessen notwendige und operationalisierende Ergänzung.

C. Der risikobasierte Ansatz als Schlüssel zur Vereinbarkeit von Datenschutz und Innovation

Der risikobasierte Ansatz ist ein prägendes, immanentes Strukturprinzip der DSGVO: Art. 24 Abs. 1 DSGVO verpflichtet Verantwortliche, die Risiken für die Rechte und Freiheiten betroffener Personen unter Berücksichtigung von Art, Umfang, Umständen und Zweck der Verarbeitung objektiv zu bewerten sowie dabei Eintrittswahrscheinlichkeit und Schwere des Risikos einzuschätzen.

I. Normative Verankerung: Risikobasierter Ansatz ist Strukturprinzip der DSGVO

Art. 25 DSGVO setzt ein risikoabhängiges Schutzniveau voraus. Art. 32 DSGVO verlangt dem Risiko angemessene technische und organisatorische Maßnahmen. Art. 35 DSGVO macht die Pflicht zur Datenschutzfolgenabschätzung (DSFA) von einem voraussichtlich hohen Risiko abhängig. Die Vorschriften zur Zulässigkeit von Drittlandsübermittlungen (Art. 44 ff. DSGVO) knüpfen ebenfalls an Risiken für betroffene Personen an, z.B. mit Blick auf geeignete Garantien.[52]

Die Ratsbegründung vom 8. April 2016 betonte ausdrücklich, dass der risikobasierte Ansatz als horizontales Strukturprinzip für sämtliche Pflichten des Verantwortlichen in

[52] Siehe auch *Paal*, NJW 2024, 3681.

die DSGVO integriert werden sollte.[53] In der Mitteilung der EU-Kommission vom 11. April 2016 wurde dieses Verständnis bestätigt, wonach der risikobasierte Ansatz dem politischen Einvernehmen entspricht, das im informellen Trilog am 15. Dezember 2015 erzielt wurde.[54] Diese Gesetzgebungshistorie wird von Behörden und Gerichten in ihrer Normanwendungspraxis allerdings bislang nicht hinreichend berücksichtigt.

Vor diesem Hintergrund werden die Potenziale des die DSGVO prägenden risikobasierten Ansatzes in der Praxis nicht hinreichend implementiert und operationalisiert. Die Datenschutzaufsichtsbehörden haben bislang kein einheitliches und ausreichendes Verständnis des risikobasierten Ansatzes entwickelt. Es fehlt ein belastbarer Konsens über Risikotaxonomie, Messung der Wahrscheinlichkeit und Schwere sowie belastbare Risikobewertungsrichtlinien. Zudem existieren in Ansehung von defizitären Governance-Strukturen[55] kaum direkte Anreize seitens der Datenschutzaufsichtsbehörden für Unternehmen, sich auf risikobasierte Rechenschaftsprogramme, Kontrollen und Instrumente entsprechend den bewerteten Risiken zu konzentrieren.[56]

Zugleich heben aber gewichtige Stimmen mit guten Gründen die Bedeutung des risikobasierten Ansatzes hervor, so etwa jüngst auch die beim Bundesministerium für Wirtschaft und Energie eingesetzte Expertenkommission „Wettbewerb & Künstliche Intelligenz“: Danach sollen „Datenverarbeitungsvorgänge mit niedrigem Risiko und geringer praktischer Identifizierungswahrscheinlichkeit [nicht] denselben umfangreichen Pflichten unterliegen wie solche mit hohem Missbrauchspotenzial“.[57]

Um den risikobasierten Ansatz als übergreifendes Strukturprinzip normativ zu verankern, sollte deshalb ein neuer Art. 5 Abs. 3 DSGVO statuiert werden, der die normative Verbindlichkeit des risikobasierten Ansatzes für Behörden und Gerichte in Ausprägung des Verhältnismäßigkeitsgrundsatzes stärkt. Erwägungsgründe sind

---

[53] Begründung des Rates: Standpunkt (EU) Nr. 6/2016 des Rates in erster Lesung im Hinblick auf den Erlass einer Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU C 159/83, S. 84. Siehe dazu auch *Paal*, ZfDR 2026, 1, 14.

[54] Mitteilung der Kommission an das Europäische Parlament gemäß Artikel 294 Absatz 6 des Vertrags über die Arbeitsweise der Europäischen Union betreffend den Standpunkt des Rates im Hinblick auf den Erlass einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr (Datenschutz-Grundverordnung) und zur Aufhebung der Richtlinie 95/46/EG, COM(2016) 214 final, S. 3 f., online abrufbar: https://www.parlament.gv.at/dokument/XXV/EU/99517/imfname_10621206.pdf.

[55] Siehe zu den Empfehlungen nachfolgend unter D. II.

[56] *Paal*, ZfDR 2026, 1, 14.

[57] Kommission „Wettbewerb & Künstliche Intelligenz“, KI, Wettbewerb & Wettbewerbsfähigkeit, 2026, S. 83.

nach ständiger EuGH-Rechtsprechung zwar für die Auslegung maßgeblich, erzeugen aber keine eigenständigen normativen Verpflichtungen. Nur ein Normtext mit operativem Regelungsgehalt wird Gerichte und Behörden zu einer systematischen Grundrechtsabwägung verbindlich verpflichten. Der Formulierungsvorschlag schafft diese normative Grundlage, ohne das materielle Schutzniveau abzusenken:[58]

*„(3) Die Grundsätze und Vorgaben dieser Verordnung zum Schutz personenbezogener Daten sind so anzuwenden und auszulegen, dass der Grundsatz der Verhältnismäßigkeit unter Berücksichtigung von Art, Umfang, Umstände und Zwecke der Verarbeitung sowie von Wahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen („risikobasierter Ansatz“) gewahrt wird. Die betroffenen Interessen, Grundrechte und Grundfreiheiten anderer als der betroffenen Person sind zu berücksichtigen; dies gilt insbesondere für unternehmerische Freiheit (Art. 16 GRCh), Wissenschafts- und Forschungsfreiheit (*Art. *13 GRCh) und Informationsfreiheit (Art. 11 GRCh). Im Kollisionsfall ist ein schonender Ausgleich der betroffenen Interessen, Grundrechte und Grundfreiheiten vorzunehmen. Ein angemessenes Schutzniveau ist zu gewährleisten. Der freie Verkehr personenbezogener Daten ist zu fördern.“*

II. Konkretisierung des risikobasierten Ansatzes I: Personenbezogene Daten

Die gemeinsame Stellungnahme von EDSA und EDSB (Joint Opinion 2/2026 vom 10. Februar 2026) zu den Digital Omnibus-Vorschlägen markiert eine wichtige Wegmarke im laufenden Reformprozess – und zwar nicht allein als Ausdruck von Widerstand, sondern als differenziertes Dokument, das eine konstruktive Auseinandersetzung ermöglicht. In zentralen Punkten (konkret der vorgeschlagenen Änderung der Personenbezugsdefinition in Art. 4 Nr. 1 DSGVO und der Rechtsgrundlage für das KI-Training) lehnen EDSA/EDSB die Digital Omnibus-Vorschläge ab oder stellen sie jedenfalls unter erheblichen Vorbehalt. In anderen Punkten hingegen – insbesondere zum vorgeschlagenen Art. 9 Abs. 5 DSGVO-E zur inzidentellen und residualen Verarbeitung besonderer Datenkategorien – signalisiert die gemeinsame Stellungnahme eine grundsätzliche Offenheit, verbunden mit dem Wunsch nach präziserer Abgrenzung und einem Dokumentationserfordernis. Dieses differenzierte Bild ist für die Reformstrategie bedeutsam, denn es zeigt, dass eine konstruktive

[58] Siehe hierzu ausführlich *Paal*, ZfDR 2026, 1, 21 sowie den Entwurf zu Art. 5 Abs. 3 DSGVO-neu der TUM-Arbeitsgruppe Datenrecht, abrufbar unter: https://tumthinktank.de/wp-content/uploads/DSGVO_RisikobasierterAnsatz_V1.pdf

Zusammenarbeit möglich ist, wenn Reformvorschläge die Präzisierungsbedarfe aufgreifen.

Der geltende Personenbezugsbegriff des Art. 4 Nr. 1 DSGVO und seine Auslegung durch den EuGH stehen im Zentrum der aktuellen Reformdebatte.[59] Das Urteil des EuGH vom 4. September 2025 (C-413/23 P – *SRB*) hat klargestellt, dass pseudonymisierte Daten nicht in jedem Fall und für jeden Beteiligten als personenbezogen gelten: Kann eine empfangende Stelle die betroffene Person mit den ihr vernünftigerweise verfügbaren Mitteln nicht re-identifizieren, fallen die übermittelten Daten für diese Stelle nicht in den Anwendungsbereich der DSGVO.

Die Joint Opinion 2/2026 von EDSA und EDSB (10. Februar 2026) hat die im Digital Omnibus vorgeschlagene Kodifizierung des relativen Personenbezugsbegriffs entschieden abgelehnt: Die Kodifizierung gehe über die EuGH-Entscheidung hinaus und schaffe neue Rechtsunsicherheiten, insbesondere durch den letzten Satz des vorgeschlagenen Textes, wonach Daten für den ursprünglichen Verantwortlichen nicht schon deshalb personenbezogen werden, weil ein nachgelagerter Empfänger über Re-Identifizierungsmittel verfügt.

Diese Ablehnung ist aus Sicht des vorliegenden Impulspapiers argumentativ zu entkräften. Der EDSA/EDSB-Einwand, die vorgeschlagene Änderung reiche über die EuGH-Entscheidung hinaus, überzeugt im Ergebnis allenfalls bedingt: Der EuGH hat in der Rs. C-413/23 P (Rn. 84-86) den kontextabhängigen Charakter des Personenbezugs und die Möglichkeit einer „relativen Anonymität“ durch Pseudonymisierung bestätigt. Es handelt sich um eine Entwicklung, die konzeptionell bereits in der Rs. C-582/14 (*Breyer*-Entscheidung) angelegt war. Eine gesetzliche Klarstellung, die diesen Gedanken systematisch in Art. 4 Nr. 1 DSGVO aufnimmt, ist geeignet, die auch von EDSA/EDSB beklagte Rechtsunsicherheit zu reduzieren, insbesondere auch, weil EDSA/EDSB, genau wie andere Aufsichtsbehörden, bis zuletzt[60] versucht hatten, an einem (möglichst) absoluten Verständnis des Personenbezugs festzuhalten. Zuzustimmen ist dem Einwand einer Gesetzesanpassung über die *SRB*-Entscheidung hinaus allenfalls (nuanciert) dahingehend, dass der Digital Omnibus-Vorschlag einen subjektiven Maßstab[61]

---

[59] Dazu auch *Paal*, GRUR 2026, 361, 364; vgl. auch COM(2025) 837 final, 23 ff.
[60] Vgl. etwa die Leitlinien 01/2025 zur Pseudonymisierung (*Guidelines 01/2025 on Pseudonymisation*), Rn. 22, die trotz mehreren Entscheidungen des EuGH mit Tendenz zu einem relativen Verständnis des Personenbezugs pseudonymisierte Daten für jeden Verantwortlichen als personenbezogen klassifizierten, sofern diese abstrakt re-identifizierbar sind; diesem Verständnis wurde mit der Entscheidung des EuGH in der Rs. 413/23 P der Boden entzogen.
[61] Vgl. die Formulierung „where that entity cannot identify”.

etablieren will, der so seine Grundlage ausdrücklich nicht in der Rechtsprechung des EuGH findet.[62]

Zugleich ist bei der Formulierung darauf zu achten, dass der letzte Satz des Digital Omnibus-Vorschlags zur Neufassung von Art. 4 Nr. 1 DSGVO (betreffend Nichtpersonenbezug bei nachgelagerter Weitergabe an re-identifizierungsfähige Dritte) präzisiert wird: Für den ursprünglichen Verantwortlichen, der die Daten an einen re-identifizierungsfähigen Empfänger übermittelt, bleiben die Daten im Moment der Übermittlung personenbezogen. Die DSGVO-Pflichten der Übermittlung, insbesondere Art. 6 und Art. 28 DSGVO, bleiben somit anwendbar. Nur für die empfangende Stelle, die selbst keine Re-Identifizierungsmöglichkeit hat, entfällt der Personenbezug. Diese Nuancierung sollte im Normtext und im zugehörigen Erwägungsgrund ausdrücklich klargestellt werden, um die Gefahr einer Umgehung der Vorschriften des Datenschutzrechts zu verhindern.

Vorzuschlagen sind nach alledem für Art. 4 Nr. 1 DSGVO verschiedene Modifikationen, die klarer differenzieren: Daten gelten für eine bestimmte Stelle nur dann als personenbezogen, wenn diese Stelle über Mittel verfügt, die vernünftigerweise zur Re-Identifizierung eingesetzt werden können, wobei ein objektivierter Horizont, nicht jedoch ein subjektiv-individueller Maßstab angelegt werden sollte. Pseudonymisierte Daten bleiben für Zwecke der Datensicherheit und der Weitergabe dann für Dritte als personenbezogen zu behandeln, wenn diese zur Re-Identifizierung fähig sind, ohne dass diese Dritten sogleich als Empfänger oder gar Verantwortliche mit der Folge einer erforderlichen Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO anzusehen sind. Dabei sollten allerdings allzu invasive Änderungen der Definition vermieden und in den Erwägungsgründen sollte festgehalten werden, dass die bislang ergangene Rechtsprechung des EuGH nicht in Frage gestellt wird, um die Gefahr zu vermeiden, dass die nun endlich eingetretene Verbesserung der Rechtssicherheit durch neue Unwägbarkeiten beeinträchtigt wird.

1. Änderungsvorschlag im Digital Omnibus in Art. 3 Abs. 1 lit. a) DSGVO:

Artikel 4 wird wie folgt geändert:

a) In Nummer 1 werden die folgenden Sätze angefügt

„Angaben zu einer natürlichen Person sind nicht notwendigerweise personenbezogene Daten für jede andere Person oder Einrichtung, nur weil eine

[62] Vgl. die *SRB*-Entscheidung des EuGH, Rn. 77 („not in a position“), s. auch Rn. 85, der abstrakter gefasst ist.

andere Einrichtung diese natürliche Person identifizieren kann; Angaben sind für eine bestimmte Einrichtung nicht personenbezogen, wenn diese Einrichtung die natürliche Person, auf die sich die Angaben beziehen, in Anbetracht der mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel, nicht identifizieren kann; derartige Angaben werden für diese Einrichtung nicht allein deshalb personenbezogen, weil ein potenzieller späterer Empfänger über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können;“

2. Eigener Änderungsvorschlag (mit Hervorhebungen)

„Angaben zu einer natürlichen Person sind nicht notwendigerweise personenbezogene Daten für jede andere Person oder Einrichtung, nur weil eine andere Einrichtung diese natürliche Person identifizieren kann; Angaben sind für eine bestimmte Einrichtung nicht personenbezogen, wenn diese Einrichtung ***nicht in der Lage ist,*** *die natürliche Person, auf die sich die Angaben beziehen, in Anbetracht der mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel,* ***zu identifizieren****; derartige Angaben werden für diese Einrichtung nicht allein deshalb* ***im Ganzen*** *personenbezogen, weil ein potenzieller späterer Empfänger über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können****, sofern eine Übermittlung an einen späteren Empfänger nicht mit hinreichender Wahrscheinlichkeit zu erwarten ist. Soweit jedoch eine Übermittlung an einen späteren Empfänger, der in der Lage ist, eine natürliche Person zu identifizieren, tatsächlich erfolgt, stellt diese Übermittlung für den Übermittler eine Verarbeitung personenbezogener Daten dar****;“*

III. Konkretisierung des risikobasierten Ansatzes II: Rechtsmissbrauch bei Betroffenenrechten

Das Betroffenenrechteregime der DSGVO birgt im KI-Kontext ein strukturelles Missbrauchspotenzial, das einer normativen Adressierung bedarf. Der EuGH hat hierzu jüngst über die Auslegung des Merkmals eines „exzessiven“ Antrags i.S.d. Art. 12 Abs. 5 S. 2 DSGVO rechtsmissbräuchlichen Auskunftsanträgen zu datenschutzfremden Zwecken zumindest teilweise einen Riegel vorgeschoben.[63]

In Ansehung von weiterhin bestehenden praktischen Schwierigkeiten, einen solchen Rechtsmissbrauch nachzuweisen, empfiehlt sich dem risikobasierten Ansatz folgend

[63] EuGH, Urt. v. 19.03.2026 – C-526/24, GRUR-RS 2026, 4080.

eine zweistufige Präzisierung: Erstens sollte Art. 12 Abs. 5 DSGVO klarstellen, dass bei nachweislich koordinierter, rein prozessmotivierter oder auf Geschäftsgeheimnisse abzielender Ausübung von Betroffenenrechten ein widerleglicher Anschein einer exzessiven Rechtsausübung gilt. Zweitens sollte in Art. 15 DSGVO normiert werden, dass das Auskunftsrecht nicht zur Umgehung des durch die Richtlinie (EU) 2016/943 und das nationale Recht gewährleisteten Geschäftsgeheimnisschutzes eingesetzt werden kann. Diese Klarstellung ist keine Einschränkung des Datenschutzes, sondern Ausdruck des in Art. 54 GRCh verankerten Verbots des Rechtsmissbrauchs.

Ergänzend empfiehlt sich für Art. 12 Abs. 5 DSGVO-E eine normative Präzisierung des Missbrauchsbegriffs.[64] Da das Verhältnis der Tatbestandsmerkmale „offenkundig unbegründet“ und „exzessiv“ zur Generalklausel der missbräuchlichen Rechtsausübung „zu anderen Zwecken als dem Schutz der Daten“ nicht hinreichend klar konturiert ist. Eine Klarstellung, wonach jene Merkmale „insbesondere“ Beispielfälle des übergeordneten Missbrauchstatbestands darstellen, würde Verantwortlichen und Gerichten einen handhabbaren Subsumtionsmaßstab an die Hand geben.

Praktisch bedeutsam ist vor allem, dass die in ErwGr. 35 DSGVO beispielhaft genannte „alleinige Absicht, dem Verantwortlichen Schaden zuzufügen“ für den Verantwortlichen nahezu unbeweisbar bleibt, solange keine Begründungspflicht für Auskunftsbegehren besteht. Ohne Begründungspflicht kann der Verantwortliche die für den Missbrauchsnachweis erforderlichen „hinreichenden Gründe“ (Art. 12 Abs. 5 S. 2 DSGVO-E) in aller Regel nicht ermitteln. Denn Informationen über den verfolgten Zweck, die die betroffene Person von sich aus nicht preisgibt, werden dem Verantwortlichen nicht vorliegen. Zur Abhilfe dienen könnte die Einführung einer gesetzlich verankerten Obliegenheit zur Zweckbenennung bei Auskunftsanträgen, die sich an ErwGr. 63 DSGVO (Selbstvergewisserung über die Rechtmäßigkeit der Verarbeitung) orientiert. Die Begründungspflicht wäre keine Einschränkung des Betroffenenrechts, sondern vielmehr Ausdruck des Verhältnismäßigkeitsgrundsatzes (Art. 52 Abs. 1 GRCh) und des Verbots des Rechtsmissbrauchs (Art. 54 GRCh).

IV. Konkretisierung des risikobasierten Ansatzes III: Rechtsgrundlagen für KI-Training und -Verwendung

Für die Frage des KI-Trainings und des KI-Einsatzes im Zusammenhang mit personenbezogenen Daten entfaltet der risikobasierte Ansatz besondere Bedeutung.

---

[64] DAV, Stellungnahme Nr. 21/2026 zum Digital-Omnibus-Vorschlag COM(2025) 837 final, März 2026 (Ausschuss Informationsrecht), S. 3–5.

Im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO ist die Wahrscheinlichkeit und Schwere einer Beeinträchtigung betroffener Personen konkret zu ermitteln. Bei einem KI-Training mit aggregierten, pseudonymisierten oder anonymisierten Daten ist das Risiko einer Beeinträchtigung individueller Persönlichkeitsrechte typischerweise gering.[65] Dies lässt die Abwägung regelmäßig zugunsten des Trainingsinteresses ausfallen.

Entscheidend kommt es dabei darauf an, den Risikobegriff nicht auf das Ausgangsrisiko einer Datenverarbeitung zu verengen, sondern darüber hinaus auch die vom Verantwortlichen bereits ergriffenen Schutzmaßnahmen in die Risikobewertung einzubeziehen.[66] Differential Privacy, Pseudonymisierung und Datensatz-Deduplikation, aber auch Maßnahmen mit Blick auf den Einsatz und die Ausgabe eines trainierten KI-Systems können das für die Interessenabwägung maßgebliche Risikoprofil erheblich senken.[67] In der Folge sinkt auch die Intensität der Compliance-Anforderungen – nicht weil der Schutz abgesenkt wird, sondern weil das tatsächliche Risiko für betroffene Personen geringer ist.

Die Interessenabwägung ist nicht auf Ebene einzelner Datenpunkte, sondern der Tätigkeit als Ganzes vorzunehmen. Bei großen heterogenen Trainingskorpora ist eine datenpunktbezogene Abwägung praktisch nicht durchführbar und auch nicht erforderlich, wenn und soweit die Tätigkeit als Ganzes die Anforderungen des Art. 6 Abs. 1 lit. f) DSGVO erfüllt.

1. Gleichrangigkeit der Rechtsgrundlagen

In der Gerichts- und Aufsichtspraxis ist die faktische Annahme einer Hierarchie zwischen den Rechtsgrundlagen des Art. 6 DSGVO zu beobachten, die eine Überhöhung der Einwilligung gegenüber anderen gleichrangigen Rechtfertigungstatbeständen bewirkt. Diese Hierarchie ist weder dogmatisch haltbar noch überhaupt sinnvoll: Art. 6 DSGVO folgt einem pluralen Legitimationsmodell, in dem keine der enumerativ aufgeführten Rechtsgrundlagen den Vorrang hat.[68] Die Einwilligung ist keine privilegierte Rechtsgrundlage für das KI-Training – insbesondere nicht, wenn massenhaft öffentlich zugängliche Daten verarbeitet werden, für die eine individuelle Einwilligung praktisch nicht einzuholen ist.

---

[65] Vgl. *Franke*, RDi 2023, 565, 568, Rn. 13, m.w.N.; *Paal*, ZfDR 2024, 129, 153.
[66] Vgl. statt vieler *Hessel/Dillschneider*, RDi 2023, 458, 461, Rn. 8; *Paal*, ZfDR 2024, 129, 153; Gola/Heckmann/*Schulz*, Art. 6 DS-GVO Rn. 63.
[67] *Paal*, ZfDR 2024, 129, 153.
[68] Statt vieler Sydow/Marsch/*Reimer*, Art. 6 DS-GVO Rn. 9.

Verstärkend tritt hinzu, dass das berechtigte Interesse nach Art. 6 Abs. 1 lit. f) DSGVO in der Aufsichtspraxis vielfach als schwache und fragile Rechtsgrundlage behandelt wird, die einer einseitig schutzorientierten Auslegung des Datenschutzgrundrechts nicht standzuhalten vermag. Dabei bildet gerade die Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO den systematischen Ort für die nach ErwGr. 4 DSGVO und Art. 52 GRCh gebotene verhältnismäßige Abwägung der Rechte, Freiheiten und Interessen bildet. Wenn und soweit die im Digital Omnibus diskutierte Standardisierung des berechtigten Interesses für KI-Entwicklungszwecke mit einer Vielzahl zusätzlicher Bedingungen verknüpft wird, droht die vermeintliche Klarstellung in der praktischen Anwendung leerzulaufen und faktisch unanwendbar zu werden. Eine zukunftsweisende Reform muss daher nicht nur eine taugliche Rechtsgrundlage benennen, sondern diese auch von einer überschießenden Bedingungslast freihalten.

Zum Zwecke der Abhilfe ist an eine Umkehrung des durch den Wortlaut implizierten Regel-Ausnahme-Verhältnisses zu denken: So könnte als Regelfall festgehalten werden, dass die Datenverarbeitung prinzipiell zuzulassen ist, wenn die Rechte und Interessen des Verarbeiters bzw. desjenigen, der ein Interesse an der Datenverarbeitung hat, diejenigen der betroffenen Person überwiegen (was strukturell Art. 6 Abs. 1 lit. f) DSGVO entspricht) und die übrigen Rechtfertigungstatbestände als dieser Grundsatzabwägung untergeordnete Regelbeispiele auszugestalten.

Zur Vermeidung einer fehlgeleiteten Hierarchisierung könnten zudem einzelne Rechtsgrundlagen in ihrem Regelungsgehalt angepasst werden. So könnte bspw. in Art. 6 Abs. 1 lit. b) DSGVO ausdrücklich klargestellt werden, dass die Notwendigkeit der Verarbeitung für die Erfüllung eines Vertrags in Bezug auf den Gegenstand des Vertragsverhältnisses zu beurteilen ist.

Schließlich ist für Art. 6 Abs. 1 lit. f) DSGVO zu erwägen, die Ausübung anderer Rechte und Freiheiten und damit verbundener Interessen in die Kategorie der berechtigten Interessen aufzunehmen, um klarzustellen, dass diese Rechtsgrundlage auch für mehrdimensionale Abwägungstests geeignet ist (z.B. mit Blick auf die zahlreichen Akteure und deren Interessen im Zusammenhang mit KI-Training). Hierdurch könnte die notwendige pluralistische Grundrechtsabwägung normativ verankert werden, die nach ErwGr. 4 DSGVO bereits *de lege lata* geboten ist. Zudem operationalisiert die Anpassung des Art. 6 Abs 1 lit. f) DSGVO die vorstehende empfohlene Verankerung des risikobasierten Ansatzes in dem hier vorgeschlagenen Art. 5 Abs. 3 DSGVO-neu.

2. Anonymisierung, Pseudonymisierung und KI

Anonymisierte Daten unterliegen nach ErwGr. 26 DSGVO nicht dem Anwendungsbereich der DSGVO. Die Anonymisierung ist nicht nur für betroffene

Personen von Bedeutung, sondern vor allem auch für Verantwortliche mit Blick auf das dann nicht mehr anwendbare Pflichtenregime der DSGVO sowie die Auflösung von Kollisionen mit anderen Rechtsakten, die wie der DA das Teilen von Daten forcieren. Dieser Befund gilt in besonderem Maße mit Blick auf nicht ohne Weiteres trennbare Mischdatensätze, wenn bereits der Personenbezug eines enthaltenen Datums den Verantwortlichen zur Einhaltung der DSGVO mit Blick auf den gesamten Datensatz veranlasst.

Darüber hinaus stellt sich bei KI-Trainingsdaten die Frage nach der Anonymisierung in spezifischer Weise: Wenn ein Trainingskorpus individuelle Datenpunkte enthält, die für sich genommen re-identifizierbar sind, das trainierte Modell aber keine Rückschlüsse auf einzelne Personen erlaubt, ist die Frage der Anonymisierung auf der Modellebene – nicht dagegen auf der Datensatzebene – zu beurteilen. Anonymisierungstechniken wie Differential Privacy können dazu beitragen, das (Rest-)Risiko einer Re-Identifizierung auf ein annehmbares Maß zu reduzieren.

Diese dogmatische Analyse ist ins Verhältnis zu setzen zu dem laufenden Gesetzgebungsverfahren. Der Digital Omnibus sieht eine kontextbezogene Identifizierbarkeitsprüfung vor: Wer selbst keine realistische Möglichkeit zur Re-Identifizierung hat, fällt grundsätzlich nicht mehr unter die DSGVO; auch das Risiko einer späteren Weitergabe an eine re-identifizierungsfähige Stelle ändert daran für den ursprünglichen Verarbeiter nichts.

Dieser Digital Omnibus-Vorschlag geht in die richtige Richtung, greift aber gleichwohl zu kurz: Denn der Vorschlag adressiert zwar den relativen Personenbezug auf Ebene des Verarbeiters, löst aber nicht das Problem der Anonymisierungspflicht als solcher – sprich die paradoxe Situation, dass der Anonymisierungsschritt selbst einer DSGVO-Rechtsgrundlage bedarf. EDSA und EDSB haben die vorgeschlagenen Änderungen an der Definition personenbezogener Daten entschieden abgelehnt, weil die Änderungen nach ihrer Auffassung den Begriff erheblich einschränken würden. Dieser Widerstand der Aufsichtsbehörden macht deutlich, dass die vollständige Umsetzung einer risikobasierten Anonymisierungsregel in der Artikel-Formulierung präzise sein muss, damit sie den EDSA/EDSB-Bedenken standhält. Eine Möglichkeit für die inhaltliche Ausgestaltung der Anonymisierung wäre, dass sie als Alternative zur Löschung eine in der DSGVO angelegte und damit bereits durch diese gerechtfertigte Datenverarbeitung darstellt. Hierdurch könnte die Anonymisierung (und damit die Zweitverwertung der nicht mehr personenbezogenen Daten) mittels einer teleologisch stimmigen Regelung auf ein belastbares Fundament gestellt werden.

Entscheidend ist jedoch, dass selbst eine überzeugende Gegenargumentation nicht hinreicht, solange der EDSA/EDSB die faktische Auslegungshoheit über zentrale DSGVO-Begriffe behält. Das strukturelle Problem ist mithin nicht allein inhaltlicher, sondern darüber hinaus vor allem auch institutioneller Natur: Die Auflösung des Widerstands der Aufsichtsbehörden gegen legislativ intendierte Reformen erfordert als notwendige Ergänzung des normativen Reformprogramms eine institutionelle Reform der Auslegungszuständigkeit (dazu sogleich unter D. III.).

Für Art. 5 Abs. 1 lit. b) DSGVO (Zweckbindung) sollte klargestellt werden, dass die Zweckbindung auch die Kompatibilität der Verarbeitung für die Zwecke der Pseudonymisierung, Anonymisierung und Erstellung anonymisierter synthetischer Daten sowie die weitere Nutzung solcher Daten umfasst. Diese Klarstellung würde die paradoxe Situation, dass der Anonymisierungsschritt selbst einer Rechtsgrundlage bedarf, auflösen, Unternehmen in ihrer Anonymisierungspraxis unterstützen und die Rechtssicherheit bei der Datenverarbeitung personenbezogener Daten stärken.

3. Besondere Datenkategorien nach Art. 9 DSGVO

Art. 9 DSGVO unterwirft besondere Datenkategorien einem Verbot mit Erlaubnisvorbehalt. Für das KI-Training besteht das Risiko, dass Trainingskorpora solche Datenkategorien zumindest implizit enthalten können. Das OLG Köln hat in einem Beschluss vom Mai 2025[69] in diesem Zusammenhang eine tätigkeitsbezogene Reduktion der Unterlassungspflicht anerkannt: Das Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO gelte nicht absolut; bei nicht zielgerichteter Verarbeitung bedürfe die Unterlassungspflicht einer näheren Konkretisierung durch einen Antrag der betroffenen Person auf Entfernung des sie betreffenden Datensatzes.

Die geltende Normkonzeption des Art. 9 Abs. 1 DSGVO ist strukturell zweifach defizitär: Sie knüpft starr an bestimmte Informationsinhalte an, ohne die Kontextabhängigkeit der Datensensibilität hinreichend abzubilden, und ordnet ein pauschales Verarbeitungsverbot an, das – namentlich im KI-Kontext – Datenverarbeitungen erfasst, bei denen keinerlei zielgerichtete Verwendung sensitiver Merkmale vorliegt.[70] Die EuGH-Rechtsprechung hat diese Defizite noch verschärft: Durch eine extensiv weite Auslegung des Tatbestands erfasst der EuGH auch mittelbar sensible Daten, ohne für die entstehenden Grenzfälle brauchbare Einschränkungskriterien zu entwickeln. Dies führt – gerade für den Einsatz von Big-

[69] OLG Köln, Urt. v. 23.5.2025 – 15 UKl 2/25, EuDIR 2025, 287.
[70] *Nabulsi*, Kontextabhängige Datensensibilität und der Anwendungsbereich von Art. 9 Abs. 1 DSGVO, Diss. 2025, S. 1 f., 73 ff.; zum Spannungsfeld zwischen Schutzzweck und Überschießen des Tatbestands ebd. S. 4 f.

Data-Technologien und KI-Trainingsdaten – zu einer normativen Überwälzung, bei der das Verarbeitungsverbot Sachverhalte erfasst, in denen erhebliche Grundrechtsrisiken für die betroffene Person objektiv nicht entstehen.[71]

De lege ferenda ist daher eine Neukonzeption des Art. 9 Abs. 1 DSGVO geboten, die den Anwendungsbereich der Vorschrift konsequent an der Kontextabhängigkeit der Datensensibilität ausrichtet: Nicht der Informationsinhalt eines Datums allein, sondern seine konkrete Risikolage im Verarbeitungskontext – unter Berücksichtigung von Informationsinhalt, Datenempfänger, Verarbeitungszweck und gesellschaftlichem Kontext – muss darüber entscheiden, ob das erhöhte Schutzregime des Art. 9 DSGVO greift.[72] Dieser Vorschlag führt auch die Verarbeitung besonderer Kategorien personenbezogener Daten konsequent auf den risikobasierten Ansatz zurück. Denn eine kontextabhängige Betrachtung bildet den Ausgangspunkt eines angemessenen Interessenausgleichs bei der Nutzung (besonderer Kategorien) personenbezogener Daten. So garantiert diese Vorgehensweise sowohl einen hohen Schutzstandard bei der Datenverarbeitung (im Lichte des deutlich verringerten Risikos bei der inzidentellen und residualen Verarbeitung) als auch die erforderliche datengetriebene Innovation im Zusammenhang mit besonderen Kategorien personenbezogener Daten.

Diese Neukonzeption ist – ihrer Tragweite entsprechend – als Maßnahme des Digital Fitness Check einzuordnen, nicht dagegen als kurzfristige Änderung im Zuge des Digital Omnibus. Für den laufenden Omnibus-Trilog genügt es, den vorgeschlagenen Art. 9 Abs. 5 DSGVO-E (inzidentelle und residuale Verarbeitung) durch präzisere Abgrenzungskriterien und ein Dokumentationserfordernis zu ergänzen; die weitergehende Reformulierung des Art. 9 Abs. 1 DSGVO bleibt dem Fitness Check vorbehalten. Hintergrund dieses zweistufigen Vorgehens ist auch, dass EDSA und EDSB in ihrer Joint Opinion 2/2026 (Rn. 46-51) dem Art. 9 Abs. 5-DSGVO-E grundsätzlich positiv gegenüberstehen, ihn aber in mehreren Punkten – namentlich der ausdrücklichen Beschränkung auf inzidentelle und residuale Verarbeitung sowie dem Dokumentationserfordernis – präzisiert sehen möchten. Diese Präzisierungen sind im Trilog umsetzbar und sollten übernommen werden. Insoweit sollte sich das Merkmal der inzidentellen und residualen Verarbeitung in Abgrenzung zu einer finalen, umfassenden Verarbeitung (z.B. mit Blick auf die Eindämmung von Bias-Risiken i.S.d. Art. 10 Abs. 5 KI-VO in der derzeitigen bzw. Art. 4a in der zukünftigen Fassung der KI-

---

[71] *Nabulsi*, S. 118 ff., 203 f.; zur Kritik an der EuGH-Rechtsprechung (C-252/21 – *Meta Platforms u.a.*; C-446/21 – *Schrems/Meta*) wegen fehlender Einschränkungskriterien und Vermengung von Tatbestands- und Rechtsfolgenseite ebd. S. 204.

[72] *Nabulsi*, S. 265 ff., 281 f.; zu den Elementen des Verarbeitungskontexts (Informationsinhalt, Datenempfänger, Verarbeitungszweck, gesellschaftlicher Kontext) ebd. S. 25 ff.

VO) ausdrücklich im Wortlaut widerspiegeln. Die Vermeidungs- und Löschungsbemühungen sollten zudem, auch im Eigeninteresse des Verantwortlichen, Gegenstand einer – mit technischen Mitteln umsetzbaren – Dokumentation sein.

Ein konsequent an der Kontextabhängigkeit der Datensensibilität orientierter Regelungsansatz muss vor diesem Hintergrund potenziell jedes sensible Datum, gegebenenfalls unter Zuhilfenahme von Clustern, einer einzelfallabhängigen Betrachtung unterwerfen. Eine Aufzählung möglicher sensibler Informationsinhalte im Gesetz darf allenfalls exemplarisch erfolgen und muss einer einzelfallabhängigen Überprüfung unterliegen – die Nennung eines Informationsinhalts in einer Sensibilitätsliste darf mit anderen Worten nicht automatisch zu der Einordnung jedes entsprechenden Datums als sensibel führen. Unter Zugrundlegung dieser Maßstäbe könnte der Wortlaut eines konsequent kontextabhängigen Regelungsansatzes lauten:[73]

„(1) Die Verarbeitung von besonders sensiblen personenbezogenen Daten ist untersagt. Besonders sensibel sind personenbezogene Daten, deren Verarbeitung im Einzelfall unter Berücksichtigung der Umstände des Verarbeitungskontexts, insbesondere des Informationsinhalts, des Datenempfängers und des Verarbeitungszwecks, erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Person herbeiführt.

(2) Besonders sensibel sind insbesondere personenbezogene Daten, aus denen sich mittelbar oder unmittelbar Informationen über die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Genetik, Sexualleben oder sexuelle Orientierung der betroffenen Person ergeben, soweit diese Daten mit der Absicht einer zweckgerichteten Verwendung des sensiblen Informationsgehalts verarbeitet werden und die sonstigen Umstände des Verarbeitungskontexts der Einordnung nicht entgegenstehen.“

4. KI-Trainingsdaten

Erhebliche Implikationen eines nicht-risikobasierten Ansatzes ergeben sich mit Blick auf das Training von KI-Modellen, die in besonderer Weise wünschenswerte Innovationen auf dem Digitalen Binnenmarkt ermöglichen können. In Ansehung des erheblichen Umfangs der benötigten Datensätze bei nur geringer Bedeutung eines einzelnen Datums für das KI-Modell können einzelne enthaltene Daten ein gesamtes

[73] *Nabulsi*, S. 270 f.

KI-Modell als nicht-datenschutzrechtskonform infizieren. Das gilt selbst dann, wenn von diesem einzelnen Datum ein kaum messbares Risiko für betroffene Personen ausgeht und der Bezug zu einer betroffenen Person allenfalls mit erheblichem Aufwand herzustellen ist. Denn gerade bei – rechtspolitisch gewollten[74] – sog. Open-Weight-Modellen ist ein unbegrenzter Personenkreis mit Blick auf die Frage einer möglichen Re-Identifizierung zu berücksichtigen.

Vor diesem Hintergrund offenbart sich die Bedeutung einerseits der zuvor vorgeschlagenen Anpassung des Art. 9 DSGVO, andererseits aber auch von DSGVO-Ausnahmetatbeständen zur Einhaltung der hohen Qualitätsanforderungen unter der KI-VO (z.B. hinsichtlich der Beseitigung unerwünschter Verzerrungen). Derartige Verzerrungen als Ausgangspunkt für eine mögliche Diskriminierung sind nach Art. 10 Abs. 1 KI-VO zu vermeiden. Zum Zwecke dieser Vermeidung kann aber wiederum gerade die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO notwendig werden. Der derzeitige Art. 10 Abs. 5 KI-VO, in seiner im Trilog konkretisierten und leicht geänderten Fassung im neuen Art. 4a, ermöglicht als Rechtsgrundlage nach Art. 9 Abs. 2 lit. g) DSGVO eine solche Datenverarbeitung. Diese gesetzliche Auflösung der Kollision zwischen DSGVO und KI-VO, anders als zwischen DSGVO und DA, ist zwar grundsätzlich begrüßenswert. Zugleich überrascht aber, dass eine derartige Erlaubnis nach dem Wortlaut nur für Hochrisiko-KI-Systeme vorgesehen ist.[75] Für alle übrigen KI-Systeme bleibt ein vergleichbarer Daten- und Systemqualitätsstandard somit regelmäßig nur theoretisch erreichbar, wenn und soweit keine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vorliegt. Ohne die wünschenswerte Klarstellung eines entsprechend weiten Anwendungsbereichs des neuen Art. 4a der KI-VO bedarf es daher mit Blick auf den Schutzzweck und die Stellung der Vorschrift im (allgemeinen) Kapitel 1 der KI-VO einer Auslegung der Vorschrift dahingehend, dass sich auch Anbieter und Betreiber von Nicht-Hochrisiko-KI-Systemen auf die Vorschrift berufen können.

5. KI-Kompetenz

Der derzeitige Art. 4 KI-VO regelt die KI-Kompetenz von Mitarbeitern, die für Betreiber sowie Anbieter von KI Systemen arbeiten: „Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz

---

[74] Siehe etwa ErwGr. 102 KI-VO.
[75] A.A. *Striebeck*, ZfDR 2026, 251, 259.

verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."

Diese Vorgabe der KI-Kompetenz ist ein belastbarer Ausgangspunkt für die Stärkung der Wettbewerbsfähigkeit und Innovationskraft des Binnenmarkts bei zugleich risikosensibler Anwendung von KI-Systemen durch den Menschen. In der derzeitigen Fassung, die im Wesentlichen unter dem Digital Omnibus erhalten bleibt, ist die Vorgabe einem risikobasierten Ansatz zugänglich und sollte auch entsprechend ausgelegt werden. Anknüpfungspunkt ist die Berücksichtigung von „their technical knowledge, experience, education and training and the context the AI systems are to be used in", die dem jeweiligen Anbieter und Betreiber in höchst unterschiedlichem Ausmaß Maßnahmen abverlangt und die jeweiligen Umstände und den KI-Einsatz umfassend berücksichtigt.

In der Trilog-Fassung findet sich zur Stärkung des risikobasierten Ansatzes in Art. 4 Abs. 1 S. 2 KI-VO die begrüßenswerte Klarstellung, dass Anbieter und Betreiber nicht „any specific level of AI literacy of any individual" garantieren müssen. Auch die Verankerung von Unterstützungsmaßnahmen der Kommission und der Mitgliedstaaten in dem neu geschaffenen Art. 4 Abs. 2 KI-VO kann zur effektiven Umsetzung beitragen und den Verantwortlichen einen Teil der Umsetzungslast abnehmen, vor allem aber etwaige Rechtsunsicherheit zur konkreten Handhabung im Einzelfall beseitigen. Entscheidend kommt es insoweit darauf an, dass derartige Unterstützungsmaßnahmen auch tatsächlich und sehr zeitnah ergriffen werden.

V. Konkretisierung des risikobasierten Ansatzes IV: Compliance-Anforderungen

1. Informationspflichten und koordinierte Dokumentation

Art. 13 und 14 DSGVO verpflichten den Verantwortlichen zur Information der betroffenen Personen über die Verarbeitung ihrer Daten. Für den KI-Einsatz entsteht eine doppelte Herausforderung: Informationspflichten bei der Datenerhebung für Trainingszwecke einerseits und Informationspflichten bei der Nutzung von KI-Systemen andererseits.

Ein pragmatischer(er) Ansatz zur Transparenz, der auf Erklärbarkeit (*explainability*) statt auf umfangreiche *ex-ante* Informationsbereitstellung setzt, könnte auch an dieser Schnittstelle entlastend wirken. Die Stärkung der Erklärbarkeit, gestützt auf den bestehenden Art. 15 DSGVO, führt zur Entlastung Verantwortlicher über

standardisierte technische Lösungen (z.B. über sog. Counterfactuals, sprich die Simulation von alternativen Eingabewerten, die zu einer anderen Ausgabe geführt hätten), während die betroffenen Personen statt einer Informationsüberlastung (sog. „information overload“) gerade die für sie besonders relevanten und aussagekräftigen Informationen im Einzelfall erhalten.

2. Art. 22 DSGVO und automatisierte Entscheidungen

KI-gestützte Einstellungsentscheidungen, Kreditvergaben oder Bonitätsbewertungen können unter Art. 22 Abs. 1 DSGVO fallen. In Hochrisiko-KI-Szenarien nach Anhang III KI-VO sind die KI-VO-Anforderungen und Art. 22 DSGVO kumulativ zu erfüllen.[76] Diese kumulative Last ist erheblich, insbesondere für Unternehmen im Bereich Human Resources und Finanzdienstleistungen.

Art. 22 Abs. 1 DSGVO schützt *de lege lata* betroffene Personen vor automatisierten Einzelfallentscheidungen, die ihnen gegenüber rechtlicher Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. In der Aufsichts- und Rechtsprechungspraxis ist die Reichweite beider Tatbestandsmerkmale bislang nicht abschließend konturiert; insbesondere das Merkmal der ähnlich erheblichen Beeinträchtigung bedarf einer klarstellenden Präzisierung, um im KI-Kontext handhabbare Maßstäbe zu schaffen.[77] Zudem führt die kumulative Anwendung von Art. 22 DSGVO und den Hochrisiko-KI-Anforderungen nach Anhang III KI-VO zu einer erheblichen Compliance-Last, die durch koordinierte Leitlinien von EDSA und EU-KI-Amt zu bewältigen ist.

Vor diesem Hintergrund ist zu erwägen, Art. 22 DSGVO mit dem nachfolgenden Absatz 2 zu ergänzen. Dieser Vorschlag grenzt den Tatbestand in zwei Richtungen präziser ein und führt die Regulierung auf risikoabhängige Bezugskriterien zurück: Erstens beschränkt er die rechtliche Wirkung auf statusbegründende oder vertragsrechtlich erhebliche Entscheidungen, womit rein vorbereitende oder empfehlende Systemausgaben ausgeschlossen werden. Zweitens macht der Vorschlag für die ähnlich erhebliche Beeinträchtigung das Kumulationsmerkmal der Dauerhaftigkeit sowie eine qualifizierte Schadensintensität (systemische Ausgrenzung, erhebliche wirtschaftliche Folgen, Entzug wesentlicher Dienste) zur Voraussetzung – dies erfolgt in Anlehnung an die Kriterien, die der EuGH in der Rs.

---

[76] *Paal/Schulz*, ZfDR 2025, 89, 100; so wohl auch *Steenbergen*, KIR 2025, 326 ff.
[77] Zum Auslegungsstreit über den Tatbestand des Art. 22 Abs. 1 DSGVO eingehend *Paal*, ZfDR 2023, 114,116 ff.; *Paal/Hüger*, MMR 2024, 540; zur Schnittstelle mit den Hochrisiko-Anforderungen der KI-VO s. oben Abschnitt C.V.2.

Schufa Holding AG für die Qualifikation eines Bonitäts-Scores als automatisierte Einzelfallentscheidung entwickelt hat.[78]

„(2) Für die Zwecke von Absatz 1 entstehen rechtliche Wirkungen nur dann, wenn die Entscheidung den rechtlichen Status einer betroffenen Person, ihre Rechte aus einem Vertrag oder vergleichbar bedeutsame Rechte maßgeblich bestimmt; und ähnlich bedeutsame Wirkungen entstehen nur dann, wenn die Entscheidung in ihrer Bedeutung einer rechtlichen Wirkung vergleichbar ist und eine dauerhafte oder permanente Einwirkung auf eine betroffene Person hat, der zu deren systemischer Ausgrenzung, erheblichen wirtschaftlichen Folgen oder dem Entzug des Zugangs zu wesentlichen Diensten führen kann."

3. DSFA und Konformitätsbewertung: Koordinierungsbedarf

Die strukturelle Überschneidung zwischen DSFA nach Art. 35 DSGVO und der Risikobewertung im Rahmen der Konformitätsbewertung nach Art. 43 KI-VO wirft komplexe Rechtsfragen mit erheblichen Rechtsunsicherheiten auf. Insbesondere für Hochrisiko-KI-Systeme, die personenbezogene Daten verarbeiten, sind beide Instrumente parallel einzusetzen,[79] was zu doppelten Dokumentations- und Prozessanforderungen führt.

Vor diesem Hintergrund sollten EDSA und EU-KI-Amt gemeinsame Leitlinien entwickeln, die eine koordinierte Durchführung von DSFA und KI-Risikobewertung ermöglichen. Bis zur Veröffentlichung entsprechender Leitlinien sollten Unternehmen ihre DSFA inhaltlich so ausgestalten, dass sie zugleich die Anforderungen des Art. 9 KI-VO an das Risikomanagementsystem abdeckt.

4. Zusammenspiel von KI-VO und sektorspezifischen Regelungen

Symptome einer Überregulierung sind mit Blick auf sektorspezifische Regelungen besonders offenkundig. So sind beispielsweise bei Spielzeugen, Medizinprodukten und Maschinen ergänzend spezifische Regeln zu beachten, die sich teils mit den Vorgaben der KI-VO überschneiden können. Diese Kumulation von Pflichten sorgt für einen deutlich erhöhten Compliance-Aufwand, dem regelmäßig kein korrespondierender Nutzen auf Seiten betroffener Personen und Nutzer gegenübersteht.

---

[78] EuGH, Urt. v. 07.12.2023, Rs. C-634/21, ECLI:EU:C:2023:957 Rn. 40 ff. – Schufa Holding AG; zur Einordnung *Paal*, ZfDR 2023, 114, 128 ff.

[79] Vgl. *Hüger/Radtke*, KIR 2025, 154, 160 sowie, ohne Bezug auf Art. 43 KI-VO, *Sachs/Meder*, ZD 2024, 363 ff. Ohne Beachtung der KI-VO, bloß auf die Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz bezogen *Schürmann*, ZD 2022, 316 ff.

Nach dem Digital Omnibus on AI-Kompromiss im Trilog sollen sektorspezifische Regelungen exklusiv und abschließend gegenüber der KI-VO zu beachten sein, soweit diese sektorspezifischen Regelungen bereits KI-Risiken adressieren. Dementsprechend werden der Maschinenverordnung (EU 2023/1230) unterfallende Systeme weitgehend vom Anwendungsbereich der KI-VO ausgenommen. Für andere sektorspezifische Regelungen kann die Kommission mit Blick auf zukünftige Harmonisierungsbestrebungen über delegierte Rechtsakte nach dem geänderten Art. 2 Abs. 13 ein entsprechendes Schutzniveau und eine nur eingeschränkte Anwendbarkeit der KI-VO feststellen.

Diese Änderungen stehen im Einklang mit der risikobasierten Adressierung von Systemen und Produkten, ohne sich überlagernde Anforderungen nach der KI-VO und dem sektorspezifischen Recht herbeizuführen. Die vorgesehene Vereinfachung der Rechtsanwendung entschärft Compliance-Aufwand bei gleichzeitiger Wahrung eines hohen KI-Schutzniveaus, wenn und soweit die sektorspezifischen Regelungen tatsächlich hinreichende Vorgaben enthalten bzw. durch delegierte Rechtsakte entsprechend ergänzt werden. Die EU-Kommission sollte die Chance nutzen, zügig für die Anwendbarkeit der KI-VO im Lichte der weiteren sektorspezifischen Regelungen die erforderliche Klarheit herzustellen und Pflichtenüberschneidungen zu verhindern

VI. Konkretisierung des risikobasierten Ansatzes V: Art. 5 DSGVO im KI-Kontext

Eine vertiefte Betrachtung der allgemeinen Verarbeitungsgrundsätze des Art. 5 DSGVO offenbart ein strukturelles Spannungsverhältnis: Die Grundsätze der Zweckbindung, Datenminimierung, Speicherbegrenzung, Richtigkeit, Transparenz und Rechenschaftspflicht sind bei einer engen Auslegung mit nahezu allen KI-Trainings- und Anwendungsszenarien nur schwer in Einklang zu bringen: Die Zweckbindung droht mit der Sekundärnutzung von Daten zu kollidieren, Datenminimierung und Speicherbegrenzung stehen in einem potenziellen Widerspruch zu Umfang und Vielfalt von Big-Data-Verarbeitungen, der Richtigkeitsgrundsatz lässt sich mit der statistisch-probabilistischen Natur von KI-Ausgaben kaum vereinbaren, und die Transparenzvorgaben stoßen wegen der *Black-Box*-Effekte bei KI an Grenzen. Ob eine Beeinträchtigung der Art. 5 DSGVO-Grundsätze vorliegt, ist einzelfallbezogen. Vor diesem Hintergrund ist im Folgenden für die einzelnen Grundsätze des Art. 5 DSGVO eine risikobasierte und verhältnismäßigkeitsorientierte Auslegung zu entwickeln. Hierzu könnte zunächst die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO um eine Verhältnismäßigkeitsklausel

ergänzt werden, die den Compliance-Nachweis auf „vernünftige Mittel unter Berücksichtigung des Ausgleichs mit anderen Rechten und Freiheiten“ begrenzt.

1. Transparenzgrundsatz

Das Transparenzprinzip nach Art. 5 Abs. 1 lit. a) DSGVO stößt im KI-Kontext auf strukturelle Grenzen. Denn der Black-Box-Effekt bei vielen KI-Systemen macht es objektiv unmöglich bzw. jedenfalls unpraktikabel, die in Art. 13-15 DSGVO geforderten Informationen bereitzustellen.[80] Der Transparenzgrundsatz sollte daher im Lichte des risikobasierten Ansatzes zur Anwendung gebracht werden, wozu konkret im Rahmen des bestehenden Auskunftsrechts stärker auf Erklärbarkeit (explainability) abgestellt werden sollte als auf *ex-ante* zu erfüllenden Informationspflichten. In diesem Zusammenhang kann auf die digitalen Transparenzvorgaben des Art. 26 DSA als mögliche Referenzmodelle und Best Practice verwiesen werden.

Diese Reformlinie findet im Digital Omnibus bereits eine erste legislative Entsprechung: Die EU-Kommission schlägt modernisierte Cookie-Regeln vor, die zu weniger Consent-Anfragen führen und es Nutzern ermöglichen, allfällige Einwilligungspräferenzen zentral in Browsern oder Betriebssystemen zu speichern. Dieser Ansatz mit einer zentralen ex-ante-Einstellung statt fragmentierter Einzelzustimmungen ist strukturell eng verwandt mit dem hier vorgeschlagenen Wechsel von überwältigenden Informationspflichten zu nachgelagerter kontextbezogener Erklärbarkeit.

Denn zweckförderliche Transparenzpflichten, die tatsächlich zu einem adäquaten Informationsstand der betroffenen Person beitragen, werden durch nachgelagerte, kontextbezogene Erklärungen dem Transparenzprinzip eher gerecht werden, als vorgelagerte Informationsfluten, die in der Praxis zumeist ungelesen bleiben. Allerdings sollte die Reform nicht dazu führen, berechtigte *ex-ante*-Informationspflichten vollständig zu beseitigen, vielmehr ist ein angemessener Ausgleich zwischen einer *ex-ante* Informationspflicht und einer *ex-post* Erklärungspflicht herzustellen.

2. Zweckbindungsgrundsatz

Weiterhin sollte der Zweckbindungsgrundsatz nach Art. 5 Abs. 1 lit. b) DSGVO so angepasst werden, dass die praxisbedeutsamen Fälle der Sekundärnutzung von Daten berücksichtigt werden, die durch die neuen rechtlichen Vorgaben der

[80] M.w.N. *Paal*, ZfDR 2024, 129, 145 f.

Europäischen Datenstrategie[81] und die künftige Strategie für eine Datenunion (Data Union Strategy)[82] sowie nationale Gesetzgebung ermöglicht werden. Konkret sollte die Kompatibilität der Verarbeitung ausdrücklich auch für öffentliche und private Forschung (mit geeigneten Garantien), für Pseudonymisierung, Anonymisierung und Erstellung anonymisierter synthetischer Daten sowie für gesetzlich vorgesehene Sekundärnutzungen gelten. In diesem Zusammenhang sollte auch die Wirkung des Art. 6 Abs. 4 DSGVO mit Blick auf die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO klargestellt werden.[83]

Die aktuell bestehende Rechtsunsicherheit über die Grenzen zulässiger Sekundärnutzung ist einer der zentralen Hemmfaktoren für KI-Innovation in Europa.[84] Unternehmen, die Daten sekundär für KI-Training verwenden möchten, operieren vielfach unter Unsicherheit und in einer normativen Grauzone.

3. Datenminimierungsgrundsatz

Zutreffend wird darauf hingewiesen, dass der Datenminimierungsgrundsatz nach Art. 5 Abs. 1 lit. c) DSGVO im Kontext der KI-Entwicklung in ein Spannungsverhältnis zu anderen Zielen treten kann: Insbesondere kann die übermäßige Minimierung einen negativen Einfluss auf die Bias-Prävention bei der Entwicklung von KI-Systemen haben. Weniger Daten bedeutet nicht automatisch bessere Daten – und nicht repräsentative Daten können zu diskriminierenden Algorithmen führen, die ihrerseits Grundrechtsverletzungen bewirken.[85]

Für Art. 5 Abs. 1 lit. c) DSGVO wird vor diesem Hintergrund daher vorgeschlagen, die Vorschrift um eine klarstellende Bestimmung zu ergänzen, wonach das Minimierungsprinzip in einer verhältnismäßigen Weise anzuwenden ist. Diese Anwendung hat ein Gleichgewicht mit anderen Rechten, Freiheiten und Interessen zu gewährleisten – dies gilt insbesondere im Hinblick auf die Verhinderung von Biases im Rahmen des KI-Trainings. Zwar gilt bei systematisch richtiger Anwendung der Datenminimierungsgrundsatz im Zusammenspiel mit dem Erforderlichkeitsgrundsatz bereits jetzt nur insoweit, als die Datenverarbeitung nicht als erforderlich anzusehen ist. Dennoch liest sich der Grundsatz *a priori* aber im Sinne einer absoluten

---

[81] COM(2020) 66 final. Dazu auch BeckOKInfoMedienR/*Debus*, 51. Edition, Stand: 01.02.2026, § 1 DNG Rn. 10 ff.; *Paal*, GRUR 2026, 361, 362 f.
[82] COM(2025) 835 final.
[83] Hierzu *Paal/Radtke*, Training eines Sprachmodells in der Justiz, 2026, S. 117.
[84] Allgemein zu den Risiken unregulierter sekundärer Nutzung *Mühlhoff/Ruschemeier*, ZfDR 2024, 337 ff.
[85] Friktionen zu den Grundsätzen der Fairness und Richtigkeit feststellend *Baumgartner/Brunnbauer/Cross*, MMR 2023, 543, 545, m.w.N. Eine geringere Qualität befürchtend *Kaulartz/Matthiesen*, RDi 2025, 141, 144, Rn. 19.

Datenminimierung, was in Ansehung von im Zeitalter der digitalen Transformation gesellschaftlich (und gesetzgeberisch) erwünschter Datennutzung (siehe insoweit insbesondere den DA) bei gleichzeitigem Schutz personenbezogener Daten nicht stimmig ist, zu einer Fehlgewichtung bei der Auslegung durch Gerichte führen kann und die Operationalisierung eines risikobasierten Ansatzes konterkariert.

Eine Speicherung von Daten für Zwecke legitimer Sekundärnutzung, Anonymisierung oder synthetischer Datengenerierung sollte ausdrücklich als zulässige Ausnahme kodifiziert werden, sofern geeignete technische und organisatorische Maßnahmen (TOMs) sowie Pseudonymisierungsmaßnahmen eingesetzt werden. Eine entsprechende Kodifikation entschärft hierbei aufgrund des erweiterten Verarbeitungskorridors nicht nur Konfliktlagen im Zusammenspiel von DA und DSGVO, sondern darüber hinaus auch Herausforderungen durch Mischdatensätze.

4. Richtigkeitsgrundsatz

Überdies sollte eine Klarstellung in Bezug auf den Richtigkeitsgrundsatz nach Art. 5 Abs. 1 lit. d) DSGVO vorgenommen werden. Dieser Grundsatz sollte auf Daten objektiver und nicht bewertender Natur beschränkt und nicht auf abgeleitete Daten ausgedehnt werden, soweit Art. 22 DSGVO nicht anwendbar ist. Hierdurch könnte vermieden werden, dass die Ergebnisse von KI-Systemen, die lediglich trend-, statistik- oder wahrscheinlichkeitsbasiert sind (und von anderen Nutzern als solche erkennbar sein dürften), stets als Verstoß gegen die allgemeinen Grundsätze angesehen werden. Die Anwendung des Genauigkeitsgrundsatzes auf KI-Ausgaben, die probabilistischer Natur sind, würde Compliance unmöglich machen oder deutlich erschweren, was wiederum dem risikobasierten Ansatz widerspricht.

5. Speicherbegrenzungsgrundsatz

In Entsprechung zu den Änderungsvorschlägen zum Zweckbindungsgrundsatz sollte zudem die zulässige weitere Speicherung auf Sekundärzwecke erstreckt werden, die durch die neuen Regelwerke der Europäischen Datenstrategie sowie nationale Gesetzgebung ermöglicht werden, sowie auf die Zwecke der Pseudonymisierung, Anonymisierung und anonymisierten Datensynthese.

D. Governance und institutionelles Design

Die Governancestruktur der europäischen Datenschutzaufsicht ist für die wirtschaftliche und unternehmerische Praxis (mit-)entscheidend. Allerdings ist die Durchsetzungspraxis europäischer Datenschutzaufsichtsbehörden stark fragmentiert, schwer vorhersehbar und in Teilen inkohärent. Unterschiedliche Auslegungsstandards zwischen nationalen Datenschutzaufsichtsbehörden, lange Verfahrensdauern und

fehlende wirtschaftliche Folgenabschätzungen beeinträchtigen die Rechtssicherheit erheblich.

Im Kern hat die institutionelle Architektur des EDSA unbeabsichtigt Anreizstrukturen geschaffen, die einen Wettbewerb um die restriktivste Position („regulatory race to the top“) begünstigen: Aufsichtsbehörden demonstrieren ihr datenschutzrechtliches Engagement durch besonders weitreichende Forderungen, während eine diffuse Verantwortungsstruktur zwischen federführender Behörde und EDSA allfällige Sanktionsmechanismen für dieses Verhalten faktisch außer Kraft zu setzen droht.

In der behördlichen Praxis äußert sich dieser Strukturmangel vielfach in einem de-facto-Absolutismus beim Datenschutz im Verhältnis zu anderen, gegebenenfalls konkurrierenden Interessen und Rechten: KI-Training wird nicht auf der Grundlage einer konkreten Risikobewertung beurteilt, sondern tendenziell pauschal als potenziell datenschutzwidrig eingestuft. Zugleich werden berechtigte Interessen nach Art. 6 Abs. 1 lit. f) DSGVO teilweise faktisch nicht als taugliche Rechtsgrundlage anerkannt. Dieser Befund begründet substanzielle Standortnachteile: Unternehmen verlegen Forschungsaktivitäten, verschieben oder streichen Investitionsentscheidungen und sehen sich mit einem regulatorischen Umfeld konfrontiert, das die Formulierung einer verlässlichen Daten- und KI-Strategie strukturell erschwert. Eine derartige Entwicklung ist insbesondere höchst bedenklich vor dem Hintergrund des Zweckes der DSGVO, eine einheitliche EU-Datenschutzregulierung zu erreichen und damit den Binnenmarkt digital zu verwirklichen.

I. Rechtsvergleich und internationale Impulse: Großbritannien

Großbritannien hat nach dem Brexit einen eigenständigen datenschutzrechtlichen Kurs eingeschlagen, der zwar strukturell an die DSGVO angelehnt bleibt, aber in wesentlichen Punkten eine innovations- und wachstumsfreundlichere Ausgestaltung verfolgt.

1. Der Data Use and Access Act 2025: Innovationsmandat für das ICO

Der Data Use and Access Act 2025 (DUAA 2025) markiert eine bedeutsame Weiterentwicklung des britischen Datenschutzrechts nach dem Brexit, wobei dem Information Commissioner's Office (ICO) eine gesetzliche Sekundärpflicht auferlegt wurde. Hiernach hat das ICO neben seinen primären Datenschutzaufgaben bei der Ausübung seiner Funktionen auch die Förderung von Innovation und Wettbewerb zu berücksichtigen (vgl. DUAA 2025, sec. 2(2)).

Die Verpflichtung zur Förderung von Innovation und Wachstum ist dabei ausdrücklich nachrangig zur primären Datenschutzmission des ICO. Somit wird gerade keine Pflicht

begründet, die Datenschutzdurchsetzung zugunsten wirtschaftlicher Interessen zurückzustellen. Es wird aber jedenfalls ein normativer Anker geschaffen, wonach das ICO bei der Entwicklung von Leitlinien, der Durchsetzungspriorisierung und der Ressourcenallokation wirtschaftliche Auswirkungen zu berücksichtigen hat.

2. Policy paper: New approach to ensure regulators and regulation support growth

Das Finanzministerium des Vereinigten Königreichs (HM Treasury) hat in diesem Papier[86] drei Maßnahmen vorgestellt, welche einen umfassenden Ansatz beschreiben, der auf drei verbundenen Reformprinzipien beruht, die einen Rückkopplungskreis aus Verantwortlichkeit, Proportionalität und Mentalitätswandel erzeugen.

Maßnahme 1: Abbau von Komplexität und Bürokratie

Unternehmerische Kosten für die Verwaltung sollen am Ende der aktuellen Legislaturperiode um 25% gesenkt worden sein. Dafür muss Bürokratie abgebaut werden. Dies verlangt zunächst eine Bestandsaufnahme aller Verwaltungskosten. Danach sollen unnötige Regelungen abgeschafft werden. Zudem sollen Behörden zusammengelegt werden, um eine Doppelarbeit zu verhindern. Ferner sollen im Bereich Umwelt und Planung Genehmigungsverfahren verkürzt werden.

Maßnahme 2: Reduzierung von Unsicherheiten bei der Regulierung

Hervorgehobenes Ziel ist die Schaffung von mehr Klarheit, Transparenz und Verlässlichkeit. Dafür müssen Dopplungen bei Regulierungsbehörden verhindert werden. Behörden müssen bei Genehmigungsverfahren zeitgebundene Zielvorgaben erstellen, an welchen sie gemessen werden. Ferner bedürfen die Umweltregulierung und das Wettbewerbsrecht einer Überarbeitung und internationale Unternehmen sollen von einem erleichterten Einstieg in das britische Finanzsystem profitieren.

Maßnahme 3: Abbau von Risikoaversionen

Im Vordergrund steht das Gleichgewicht von Verbraucherschutz und Wachstumsförderung. Das neu installierte Regulatory Innovation Office (RIO) soll regulatorische Hindernisse abbauen und einen kulturellen Wandel fördern. In mehreren Zukunftsbereichen wird das RIO aktiv werden. Zudem sollen insgesamt auch Regulierungsbehörden KI-Innovation ermöglichen.

---

[86] Online abrufbar: https://www.gov.uk/government/publications/a-new-approach-to-ensure-regulators-and-regulation-support-growth/new-approach-to-ensure-regulators-and-regulation-support-growth-html#action-1-tackle-complexity-and-the-burden-of-regulation.

3. Übertragbarkeit auf das europäische Datenschutzrecht

Die zentrale (rechtliche) Frage ist, ob und welche dieser Konzepte auf den europäischen Datenschutzbereich übertragen werden können, ohne die Unabhängigkeit der Datenschutzaufsichtsbehörden nach Art. 51 ff. DSGVO zu gefährden.

Art. 52 Abs. 1 DSGVO verlangt zwar vollständige Unabhängigkeit der Datenschutzaufsichtsbehörden bei der Ausübung ihrer Aufgaben, schreibt aber nicht vor, dass Datenschutzaufsichtsbehörden von jeglicher demokratischen Rechenschaftspflicht freigestellt sind. So liegt die Überprüfung von selbst aufgestellten Zielvorgaben im rechtlich erlaubten Rahmen. Die Einrichtung eines beratenden Gremiums mit rein konsultativem Status gefährdet die Unabhängigkeit nicht, sondern stärkt vielmehr die institutionelle Kapazität.

Zugleich bedarf es eines belastbaren Transparenz- und Rechenschaftsmechanismus. Denn es wird nicht genügen, Datenschutzaufsichtsbehörden zur Berücksichtigung von Innovation und Wettbewerbsfähigkeit zu verpflichten; erforderlich ist darüber hinaus, dass diese Berücksichtigung nach außen sichtbar und nachprüfbar wird.

Konkret sollten Datenschutzaufsichtsbehörden durch regelmäßige, veröffentlichte Berichte darlegen, wie sie ihre Entscheidungen getroffen haben, wie dabei eine ausgewogene Abwägung zwischen Datenschutz, Innovation und wirtschaftlicher Entwicklung vorgenommen wurde, welche Positionen sie im EDSA vertreten haben und wie europäische Leitlinien in die nationale Praxis überführt wurden. Diese Transparenzpflicht schützt die Unabhängigkeit, weil sie keine inhaltlichen Entscheidungsvorgaben macht, und erzeugt zugleich eine Rechenschaftspflicht, die bislang strukturell fehlt.

Im nationalen Reformkontext ist zu betonen, dass Deutschland den EU-Gesetzgebungsweg nicht abwarten muss. Eine BDSG-Novelle könnte Deutschland als erstes großes EU-Mitglied positionieren, das seiner Datenschutzaufsichtsbehörde ein gesetzliches Innovationsmandat erteilt. Hierbei würde es sich um einen Präzedenzfall mit Impulskraft für vergleichbare Reformen in anderen Mitgliedstaaten handeln. Die im Koalitionsvertrag 2025 der Bundesregierung vorgesehene Umbenennung der Durchsetzungs- und Beratungspraxis der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) (wobei hiermit grundsätzlich keine Änderung der Rechtsstellung begründet wird) droht jenseits der Symbolkraft wirkungslos zu bleiben, wenn das gesetzliche Mandat weiterhin ausschließlich auf Datenschutz ausgerichtet ist.

Zum Abbau von Komplexität und Überregulierung durch nationale Gesetzgebung, die über die europäischen Vorgaben hinausgeht („Gold-Plating“), könnten im Zuge einer BDSG-Novelle die nationalen Vorgaben auf eine 1:1-Umsetzung der DSGVO-Vorgaben zurückgebaut werden.

Das hier vorgeschlagene Reformprogramm setzt deshalb auf vier normative Maßnahmen im BDSG: Erstens eine Überprüfung und Verschlankung des BDSG auf das durch die DSGVO vorgegebene angemessene Schutzniveau. Zweitens eine sekundäre gesetzliche Pflicht der BfDI zur Förderung von Innovation und Wirtschaftswachstum – ausdrücklich unter Wahrung des primären Datenschutzmandats, um die Vereinbarkeit mit Art. 51 Abs. 1 DSGVO sicherzustellen, und in Fortsetzung der im Jahr 2025 begonnenen Neuausrichtung der BfDI. Drittens eine kennzahlenbasierte Berichtspflicht über die Auswirkungen der Leitlinienpraxis und Vollzugstätigkeit auf Innovation und Wettbewerbsfähigkeit. Viertens die Einrichtung einer unabhängigen „Wachstums- und Innovationskommission bei der BfDI“, die strukturierte Sachverständigenberatung aus Wirtschaft, Technologie und Wissenschaft institutionalisiert. Vorbilder finden sich – wie vorstehend bereits ausgeführt – im Growth and Investment Council der Competition and Markets Authority (CMA) sowie in den Practitioner Panels der Financial Conduct Authority (FCA). Diese drei Maßnahmen bewegen sich zudem im nationalen Regelungsraum des Art. 57 Abs. 1 DSGVO und bedürfen keinerlei Abweichung vom Unionsrecht. Auf Basis dieser Anpassungen erleichtert eine teilweise geforderte[87] Zentralisierung der Datenschutzaufsicht die konsequente Fortführung dieses Kurses und die Zusammenbringung von Datenschutz und Datennutzung in einer Hand.

II. Innovationspflicht für Datenschutzaufsichtsbehörden

Art. 57 DSGVO regelt die Aufgaben der Datenschutzaufsichtsbehörden und ist ausschließlich schutzorientiert formuliert.[88] Zugleich fehlt es an einer hinreichenden Verpflichtung, wirtschaftliche Auswirkungen von Leitlinien und Durchsetzungsmaßnahmen zu berücksichtigen.[89] Im Vergleich mit sektorspezifischen Regulierungen – insbesondere dem Finanzmarktrecht, in dem Aufsichtsbehörden

[87] Kommission Wettbewerb & Künstliche Intelligenz, KI, Wettbewerb & Wettbewerbsfähigkeit, 2026, S. 84 f.
[88] Kühling/Buchner/*Boehm*, 4. Aufl. 2024, Art. 57 DSGVO Rn. 1, 2; Paal/Pauly/*Körffer*, 4. Aufl. 2026, Art. 57 DSGVO Rn. 1; Sydow/Marsch/*Ziebarth*, 3. Aufl. 2022, Art. 57 DSGVO Rn. 2, 3.
[89] Dies wohl teilweise in Art. 57 Abs. 1 lit. i) DSGVO verankernd Simitis/Hornung/Spiecker gen. Döhmann/*Polenz*, 2. Aufl. 2025, Art. 57 DSGVO Rn. 38.

ausdrücklich zur Berücksichtigung der Marktfunktionsfähigkeit verpflichtet sind – besteht für die DSGVO eine auffällige Asymmetrie.

Insoweit bietet es sich an, für allgemeine Entscheidungsentwürfe und Leitlinien sowie für Entscheidungen mit repressiver Natur die Aufsichtsbehörde zu verpflichten, vorab eine Folgenabschätzung zu den Auswirkungen solcher Entscheidungen auf Innovation und Wettbewerbsfähigkeit vorzunehmen. Diese Folgenabschätzung sollte unter anderem auch die Wissenserweiterung und den Technologietransfer sowie andere öffentliche Interessen, Grundrechte und Grundfreiheiten berücksichtigen sowie veröffentlicht werden.

Eine Umsetzung dieses Vorschlags empfiehlt sich in einem neuen Art. 57 Abs. 1a DSGVO. Die Formulierung sollte klarstellen, dass die wirtschaftliche Folgenabschätzung die primäre Datenschutzaufgabe der Datenschutzaufsichtsbehörden nicht einschränkt, sondern lediglich eine zusätzliche Überprüfungspflicht begründet. Die nachfolgend vorgeschlagene Formulierung ist dem DUAA 2025-Vorbild nachgebildet, in der Terminologie des europäischen Datenschutzrechts verankert und schafft einen normativen Anker für eine systematische Berücksichtigung wirtschaftlicher Auswirkungen ohne Gefährdung der verbürgen Unabhängigkeit der Datenschutzaufsichtsbehörden. Die Pflicht zur Veröffentlichung der wirtschaftlichen Folgenabschätzung gewährleistet Transparenz und demokratische Rechenschaftspflicht.

„Art. 57 (1a) DSGVO-neu: Bei der Wahrnehmung ihrer Aufgaben nach dieser Verordnung hat die Aufsichtsbehörde das Ziel der Förderung von Innovation und Wettbewerb zu berücksichtigen, soweit dies mit dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten vereinbar ist. Zu diesem Zweck hat die Aufsichtsbehörde für Leitlinien, Codes of Conduct und Durchsetzungsmaßnahmen eine wirtschaftliche Folgenabschätzung zu erstellen und zu veröffentlichen.“

III. Konsultationspflichten für EDSA und nationale Datenschutzaufsichtsbehörden

Zudem sollten auf EU-Ebene verbindliche Normen für Beteiligungsverfahren vor Entscheidungen und Leitlinien der Datenschutzaufsichtsbehörden eingeführt werden. Dies umfasst eine bindende Bestimmung, wonach Datenschutzaufsichtsbehörden verpflichtet sind, bei ihren Entscheidungen und Leitlinien partizipatorische Vorab-Konsultationsverfahren einzuleiten, die Festlegung gemeinsamer Grundsätze zur Gewährleistung der Konsistenz der nationalen Konsultationsmodelle sowie für den

EDSA die Verpflichtung, interessierte Parteien zu konsultieren und diesen Gelegenheit zu geben, innerhalb einer angemessenen Frist Stellung zu nehmen.

Die vorgeschlagenen Konsultationspflichten sind darüber hinaus vereinbar mit der Unabhängigkeit der Datenschutzaufsichtsbehörden nach Art. 51 ff. DSGVO, die allein die Entscheidungsautonomie der Behörden schützt, nicht aber deren demokratische Rechenschaftspflicht ausschließen soll.[90] Konsultationspflichten sind strukturell vergleichbar mit den in anderen Regulierungsbereichen (z.B. dem Finanz- und Telekommunikationsrecht) etablierten Verfahren.

Die Konsultationspflicht sollte dabei nicht auf die Beteiligung betroffener Kreise beschränkt bleiben, sondern um eine behördenübergreifende Komponente ergänzt werden: In Ansehung des neuen unionsrechtlichen Rahmens (i.e. DA, DGA, Verordnungen zu gemeinsamen Datenräumen, KI-VO) sollten die Datenschutzaufsichtsbehörden verpflichtet werden, vor dem Erlass allgemeiner wie einzelfallbezogener Maßnahmen die jeweils fachlich zuständigen unabhängigen Behörden (etwa für Datenverwaltung, KI, Cybersicherheit, Finanzwesen sowie Gesundheit und Forschung) zu konsultieren und deren Stellungnahmen einzuholen. Eine solche sektorübergreifende Abstimmung ergänzt die vorstehend (unter D.II) vorgeschlagene wirtschaftliche Folgenabschätzung in funktionaler Hinsicht: Während die Folgenabschätzung die Auswirkungen auf Innovation und Wettbewerbsfähigkeit transparent macht, sichert die behördenübergreifende Konsultation die fachliche Kohärenz der Aufsichtspraxis im ebenso komplexen wie zunehmend verflochtenen Digital Acquis und beugt isolierten, allein datenschutzzentrierten Bewertungen vor.

IV. Herstellung datenrechtlicher Kohärenz

Im Digital Omnibus sollen der DGA, die Free-Flow-of-Data-VO und die Offene Daten-RL in den DA integriert werden.[91] Damit lässt sich in begrüßenswerter Weise nicht nur Rechtssicherheit, sondern auch die notwendige Kohärenz herstellen.

Diese Kohärenz muss darüber hinaus aber auch für das Zusammenspiel von DA und DSGVO erreicht werden. Hierfür bedarf es nicht zwingend einer Zusammenführung der Rechtsakte, sondern vielmehr (nur) der Identifizierung und Adressierung von Friktionen und der hierdurch erzeugten Konfliktlagen. Dies kann beispielsweise durch die vorstehend vorgeschlagenen Anpassungen der DSGVO mit Blick auf den risikobasierten Ansatz[92] erreicht werden. Darüber hinaus empfiehlt sich eine Auflösung

---

[90] Ehmann/Selmayr/*Selmayr*, 3. Aufl. 2024, DS-GVO Art. 52 Rn. 10, Fn. 55.
[91] Hierzu *Striebeck*, ZfDR 2026, 251, 272 m.w.N.
[92] Siehe hierzu vorstehend unter C.

des Spannungsverhältnisses zwischen DA und DSGVO durch den Gesetzgeber. Denkbar wäre z.B. im DA in Abkehr von ErwGr. 7 S. 7 DA ausdrücklich eine Pflicht zur Verarbeitung personenbezogener Daten im Zusammenhang mit Art. 3 ff. DA zu verankern, die sodann als eine Rechtsgrundlage i.S.d. Art. 6 Abs. 1 lit. c) DSGVO herangezogen werden könnte.

Gangbare Wege zur Auflösung eines Spannungsverhältnisses zwischen der DSGVO und weiteren Rechtsakten demonstriert der KI-Omnibus in der Trilog-Fassung: Die KI-VO kann demnach nicht nur eine Rechtsgrundlage i.S.d. DSGVO darstellen (siehe Art. 4a; zuvor Art. 10 Abs. 5 KI-VO), sondern Dokumentationspflichten nach beiden Rechtsakten werden unmittelbar miteinander verschränkt (siehe den neuen Art. 27 Abs. 4 mit Blick auf die Grundrechte-Folgenabschätzung nach der KI-VO und die DSFA nach der DSGVO).

E. Zusammenfassung der wesentlichen Ergebnisse und Handlungsempfehlungen

Die nachfolgenden Ergebnisse und Handlungsempfehlungen geben Antworten auf die Leitfrage des Impulspapiers: „Wo müssen wir mit Blick auf das Datenrecht ansetzen, um die Nutzung und Entwicklung von KI in Unternehmen zu erleichtern?“ Die nachfolgenden Ausführungen sind als konsolidierte Reformimpulse für den Digital Omnibus und den Digital Fitness Check zu verstehen und verfolgen das übergeordnete Ziel einer strategischen Weiterentwicklung des europäischen Digital Acquis, die Grundrechtsschutz und Innovationsförderung, Wettbewerbsfähigkeit und digitale Souveränität als gleichrangige Ziele verwirklicht.

Erstens verletzt der Null-Risiko-Ansatz die aus Art. 8 GRCh, Art. 52 Abs. 1 GRCh und ErwGr. 4 DSGVO folgende Abwägungspflicht. Das Grundrecht auf Datenschutz ist kein absolutes Recht. Datenverarbeitungen zu KI-Zwecken sind unter Inbezugnahme (unter anderem) der unternehmerischen Freiheit nach Art. 16 GRCh und des gemeinwohlbezogenen Innovationsinteresses in eine normbezogene Güterabwägung einzustellen. Diese Güterabwägung hat sich unter Berücksichtigung von Verhältnismäßigkeit auf die Herstellung von praktischer Konkordanz und einen schonenden Ausgleich kollidierender Interessen und Rechtsgüter auszurichten. Zur normativen Absicherung dieser Abwägungspflicht empfiehlt sich – unter anderem – eine Ergänzung von Art. 1 DSGVO um ein explizites Innovationsmandat (Art. 1 Abs. 3a DSGVO-neu), das Innovation, digitale Entwicklung und Wettbewerbsfähigkeit der Union als gleichrangige Ziele neben dem Datenschutz verankert.

Zweitens ist Art. 6 Abs. 1 lit. f) DSGVO (berechtigte Interessen) im Grundsatz eine geeignete Rechtsgrundlage für die Verarbeitung öffentlich zugänglicher (personenbezogener) Daten im Rahmen des KI-Trainings. Die vorzunehmende Interessenabwägung wird bei anonymisierten oder pseudonymisierten Trainingsdaten vielfach zugunsten des Trainingsinteresses ausfallen. Es besteht keine normative Hierarchie zwischen den Rechtsgrundlagen des Art. 6 DSGVO; die Einwilligung ist weder die einzige noch eine privilegierte Rechtsgrundlage für das KI-Training. Technische Schutzmaßnahmen (insbesondere Differential Privacy, Pseudonymisierung und Datensatz-Deduplikation) senken das Risikoprofil einer KI-Verarbeitung und sind als positive Faktoren sowohl in für die Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO als auch für die Datenschutzfolgenabschätzung nach Art. 35 DSGVO heranzuziehen.

Drittens ist der risikobasierte Ansatz einer der zentralen normativen Hebel für eine innovationsfreundlichere Auslegung der DSGVO. Dieser risikobasierte Ansatz ist als Strukturprinzip bereits *de lege lata* in der DSGVO angelegt und sollte *de lege ferenda* als übergreifendes Grundprinzip an zentraler Stelle im Normtext verankert werden. In diesem Sinne empfiehlt sich ein pragmatischer, innovations- und verhältnismäßigkeitsorientierter Neuansatz für DSGVO-Kernprinzipien, Erlaubnistatbestände und die Governance-Architektur der Aufsichtsbehörden. *De lege ferenda* kann dies etwa durch eine ausdrückliche Verankerung des risikobasierten Ansatzes in Art. 5 Abs. 3 DSGVO-neu geschehen.

Viertens erzeugt das Nebeneinander von DSGVO-Pflichten, Vorgaben der KI-VO und weiterer Digitalrechtsakte, wie bspw. des DA, an zentralen Schnittstellen kumulierte Compliance-Lasten, die insbesondere für KMU kaum mehr beherrschbar und umsetzbar sind. Koordinierte Leitlinien, Orientierungshilfen und belastbare Handreichungen zur Gesetzesanwendung sind deshalb dringend geboten. Hierbei sind konkret zwei Schnittstellen vorrangig zu adressieren: (1) Die strukturelle Überschneidung von DSFA (Art. 35 DSGVO) und KI-Konformitätsbewertung (Art. 43 KI-VO) erfordert gemeinsame Leitlinien für eine koordinierte Durchführung. (2) Die kumulative Anwendung von Art. 22 DSGVO und den Hochrisiko-KI-Anforderungen nach Anhang III KI-VO bei automatisierten Entscheidungen ist auf ein handhabbares Maß zurückzuführen.

Fünftens erfordert die Wirksamkeit des normativen Reformprogramms eine Reform der Auslegungshoheit auf EU-Ebene. Selbst eine überzeugende dogmatische Gegenargumentation gegen restriktive EDSA/EDSB-Positionen – etwa zur Personenbezugsdefinition nach Art. 4 Nr. 1 DSGVO oder zur Rechtsgrundlage für das

KI-Training nach Art. 6 Abs. 1 lit. f) DSGVO – kann nicht verhindern, dass der EDSA legislative Reformabsichten durch seine Auslegungspraxis faktisch unterläuft, solange er die primäre Interpretationshoheit über abstrakt-generelle DSGVO-Begriffe innehat und diese Kompetenz gerichtlich nicht unmittelbar anfechtbar ist. Das strukturelle Problem ist mithin nicht allein inhaltlicher, sondern vor allem auch institutioneller Natur.

F. Handlungsmatrix: Digital Omnibus-Sofortmaßnahmen und Fitness-Check-Reformziele

Die Zweistufenarchitektur der EU-Digitalrechtsreform (i.e. Digital Omnibus für punktuelle Sofortmaßnahmen und Digital Fitness Check für strukturelle Systemkorrekturen) erfordert eine Zuordnung der vorliegend entwickelten Handlungsempfehlungen.

Die nachstehende Übersicht gibt hierfür eine erste Orientierung:

I. Stufe 1: Digital Omnibus

- Klarstellung des relativen Personenbezugsbegriffs in Art. 4 Nr. 1 DSGVO unter Berücksichtigung der EuGH-Entscheidung in der Rs. C-413/23 P (*SRB*) und mit präziser Formulierung des Übermittlungsszenarios (dazu oben C.II.).

- Klarstellung der Gleichrangigkeit der Rechtsgrundlagen des Art. 6 DSGVO und Aufnahme von Art. 6 Abs. 1 lit. f) DSGVO als taugliche Rechtsgrundlage für das KI-Training in einem ergänzenden Erwägungsgrund (dazu oben C.IV.1).

- Ergänzung von Art. 9 Abs. 5 DSGVO-E (inzidentelle und residuale Verarbeitung besonderer Datenkategorien im KI-Kontext): Konkretisierung des Anwendungsbereichs und Aufnahme eines Dokumentationserfordernisses für den Nachweis der Unmöglichkeit der Löschung (dazu oben C.IV.3).

- Präzisierung des Tatbestands des Art. 22 Abs. 1 DSGVO durch Ergänzung eines neuen Abs. 2, der den Begriff der rechtlichen Wirkung auf statusbegründende oder vertragsrechtlich erhebliche Entscheidungen beschränkt und für die ähnlich erhebliche Beeinträchtigung das Merkmal der Dauerhaftigkeit sowie eine qualifizierte Schadensintensität zur Voraussetzung macht (dazu oben C.V.2).

- Präzisierung von Art. 12 Abs. 5 DSGVO betreffend Rechtsmissbrauch (dazu oben C.III).

II. Stufe 2: Digital Fitness Check

- Aufnahme eines Innovationsmandats in Art. 1 Abs. 3a DSGVO-E und normative Verankerung des risikobasierten Ansatzes in Art. 5 Abs. 3 DSGVO-E (dazu oben A.V, B.III, C.I).
- Neukonzeption des Art. 9 Abs. 1 DSGVO auf der Grundlage und am Maßstab eines konsequent kontextabhängigen Sensibilitätsbegriffs (dazu oben C.IV.3).
- Einführung einer Pflicht zur wirtschaftlichen Folgenabschätzung für DSGVO-Leitlinien in Art. 57 Abs. 1a DSGVO-E sowie verbindliche Konsultationspflichten für EDSA und nationale Datenschutzaufsichtsbehörden (dazu oben D.II, D.III).
- Koordinierung von DSFA (Art. 35 DSGVO) und KI-Konformitätsbewertung (Art. 43 KI-VO) sowie Informationspflichten (Art. 13, 14 DSGVO) durch gemeinsame Leitlinien von EDSA und EU-KI-Amt (dazu oben C.V.1 und C.V.3).

IHK München und Oberbayern

Impressum

Verleger und Herausgeber:
IHK für München und Oberbayern
Dr. Manfred Gößl
Max-Joseph-Straße 2, 80333 München
089 5116-0
info@muenchen.ihk.de
ihk-muenchen.de

Ansprechpartner:
Franziska Neuberger
Referatsleiterin Digitalisierung und IKT
089 5116-0
neuberger@muenchen.ihk.de

Chantal Berier
Referentin für Digitalpolitik
089 5116-0
berier@muenchen.ihk.de

Autor/–innen:
Prof. Dr. Boris Paal, M. Jur. (Oxford)
Technische Universität München
boris.paal@tum.de

Gestaltung Umschlag:
Ideenmühle GmbH, Eckental

Bildnachweis:
Titel: Adobe Stock © champpixs

Stand: Juni 2026