

Der EU-Digital-Omnibus Änderung von DS-GVO und KI-Verordnung

I. Einleitung

Die Europäische Kommission verfolgt mit dem sogenannten Digital-Omnibus das Ziel, zentrale Regelwerke des europäischen Digitalrechts zu vereinfachen, besser aufeinander abzustimmen und Bürokratie zu reduzieren. Betroffen sind insbesondere die Datenschutz-Grundverordnung DS-GVO und die KI-Verordnung, daneben auch weitere Digitalrechtsakte wie das ePrivacy-Regime und Teile des Datenrechts.

Für die wissenschaftliche Einordnung ist der Omnibus weniger als bloßes „Aufräumgesetz“ zu verstehen, sondern als regulierungspolitische Weichenstellung auf europarechtlicher Ebene. Denn die geplanten Änderungen berühren nicht nur Verfahrensfragen, sondern auch Grundbegriffe des Datenschutzrechts und die Systematik der risikobasierten KI-Regulierung.

II. Begriff und Einordnung

Unter einem „Omnibus“-Verfahren versteht man gesetzgeberische Sammeländerungen, mit denen mehrere Rechtsakte in einem Paket angepasst werden. Im Digitalbereich nutzt die Kommission dieses Instrument, um die wachsende Zahl an Parallelregimen – insbesondere DS-GVO, Data Act, Data Governance Act und KI-Verordnung – besser zu verzahnen.

Das politische Leitmotiv lautet dabei: Vereinfachung. Gleichzeitig zeigen die vorliegenden Stellungnahmen, dass zwischen Vereinfachung und materieller Absenkung des Schutzniveaus eine schmale Grenze verläuft. Genau an dieser Stelle entstehen die zentralen Konflikte des Vorhabens.

III. Historischer Hintergrund

Die europäische Digitalregulierung ist in den letzten Jahren schrittweise und teils nebeneinander entstanden. Dadurch sind Überschneidungen, Abgrenzungsprobleme und Doppelpflichten entstanden, etwa zwischen Datenschutzrecht und KI-Regulierung als Produktrecht.

Die EU-Kommission reagiert darauf mit dem Digital-Omnibus und will bestehende Regelwerke stärker harmonisieren. Der Vorschlag wurde am 19. November 2025 veröffentlicht (COM/2025/837 final) und befindet sich seither im europäischen Gesetzgebungsverfahren.

IV. Zielsetzung des Omnibus

Das Vorhaben verfolgt vor allem drei Ziele: weniger bürokratische Lasten, mehr Rechtssicherheit und bessere Anschlussfähigkeit zwischen den Digitalrechtsakten. Unternehmen sollen nach dem Willen der Kommission klarer erkennen können, welche Regeln wann gelten.

Zugleich soll Innovation gefördert werden, insbesondere bei datengetriebenen Geschäftsmodellen und KI-Anwendungen. Die Vorlagen zeigen jedoch, dass dieser Innovationsimpuls teilweise mit einer Neugewichtung des Datenschutzes und der KI-Aufsicht einhergehen könnte.

V. Änderungen an der DS-GVO

1. Neue Definition von personenbezogenen Daten

Besonders umstritten ist die geplante Präzisierung des Begriffs der personenbezogenen Daten (aktuell geregelt in Art. 4 Nr. 1 DS-GVO). Die Kommission will den Personenbezug stärker relativieren und auf die Perspektive des jeweiligen Datenempfängers beziehungsweise der konkreten Stelle abstellen.

Die EDPB/EDPS-„Joint Opinion“ (Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter) kritisiert dies scharf und betont, dass eine solche Änderung den Kernbereich des Datenschutzrechts betreffe. Nach ihrer Auffassung würde der Vorschlag den Anwendungsbereich der DS-GVO spürbar verengen und über eine bloße Kodifizierung der EuGH-Rechtsprechung hinausgehen.

2. Bedeutung der EuGH-Rechtsprechung

Die Kommission stützt ihre Linie auf die EuGH-Entscheidung in der Rechtssache C-413/23 P, in der der Gerichtshof die Identifizierbarkeit aus Sicht des jeweiligen Empfängers betont hat. Gleichzeitig lässt sich aus der Stellungnahme der Aufsichtsbehörden ableiten, dass die unionsrechtliche Rechtsprechung nicht auf eine einseitige Verengung des Personenbegriffs reduziert werden darf.

Gerade die juristische Bewertung im Digitalen Omnibus, Informationen würden nicht allein deshalb personenbezogen, weil ein späterer Empfänger sie identifizieren könne, wird als problematisch bewertet. Die Aufsichtsbehörden sehen darin das Risiko, dass Unternehmen Datenströme künstlich so strukturieren, dass sie aus dem Anwendungsbereich der DS-GVO herausfallen.

3. Pseudonymisierung und Implementing Acts

Ein weiterer sensibler Punkt ist die geplante Ermächtigung der Kommission, durch Durchführungsrechtsakte zu bestimmen, wann pseudonymisierte Daten für bestimmte Stellen nicht mehr als personenbezogen gelten. Die Aufsichtsbehörden halten dies für systemwidrig, weil damit die Abgrenzung des Anwendungsbereichs des Datenschutzrechts faktisch an die Europäische Kommission als Organ der Exekutive verlagert würde.

Aus wissenschaftlicher Sicht ist das ein klassischer Konflikt zwischen Flexibilisierung und Normklarheit. Je stärker die Kommission die Grenzziehung zwischen anonymen und personenbeziehbaren bzw. personenbezogenen Daten auslagert, desto größer wird das Risiko uneinheitlicher Anwendung und normativer Unsicherheit.

4. Forschung, Transparenz und Datenzugang

Neben den umstrittenen Kernfragen enthält der Entwurf auch tendenziell konsensfähige Elemente, etwa im Bereich wissenschaftlicher Forschung. Die Joint Opinion begrüßt unter anderem die geplante Definition, die Klarstellung zu Art. 6 Abs. 4 DS-GVO und punktuelle Erleichterungen bei der Informationspflicht.

Auch beim Umgang mit sog. Datenpannen (Art. 33 DS-GVO) und Datenschutz-Folgenabschätzungen (Art. 35 DS-GVO) werden Vereinfachungen grundsätzlich positiv gesehen, sofern sie die Rechtssicherheit erhöhen. Die EDPB/EDPS betonen jedoch, dass solche Erleichterungen nur dann tragfähig sind, wenn sie die Unabhängigkeit der Aufsichtsbehörden und den Grundrechtsschutz nicht schwächen.

5. Biometrie und besondere Datenkategorien

Der Entwurf enthält zudem eine neue Ausnahme für die Verarbeitung biometrischer Daten i.S.d. Art. 9 DS-GVO zur Authentifizierung, sofern die Verifikationsmittel unter der alleinigen Kontrolle der betroffenen Person stehen. Diese Linie wird in der Joint Opinion eher wohlwollend aufgenommen, allerdings unter dem Vorbehalt klarer Schutzmechanismen.

Für besondere Datenkategorien im KI-Kontext sieht die Kommission außerdem eine begrenzte Ausnahme für unbeabsichtigte oder residuale Verarbeitung vor. Die Aufsichtsbehörden akzeptieren den praktischen Bedarf teilweise, verlangen aber präzisere Voraussetzungen, engere Schranken und wirksame Löscho- und Sicherungsmechanismen.

6. Rechte betroffener Personen

Bei den Betroffenenrechten will der Omnibus unter anderem missbräuchliche Auskunftsanträge stärker begrenzen und Transparenzpflichten in bestimmten Konstellationen lockern. Auch dies wird grundsätzlich als nachvollziehbares Ziel angesehen, solange die Einschränkungen eng bleiben und nicht zu einer faktischen Entwertung der Rechte führen.

Die Joint Opinion warnt jedoch davor, den Begriff der rechtsmissbräuchlichen Anwendung von Betroffenenrechten zu weit zu fassen. Das Recht auf Auskunft sei nicht nur ein Datenschutzinstrument, sondern auch ein Mittel zur Wahrnehmung anderer Grundrechte und Freiheiten.

VI. Änderungen an der KI-Verordnung

1. Fristen und Compliance

Für die KI-Verordnung enthält der Omnibus beziehungsweise das separate KI-Änderungspaket vor allem Fristverlängerungen für bestimmte Hochrisiko-Systeme. Für Anbieter und Betreiber von KI-Systemen sollen die Fristen zur Anwendungspflicht teilweise nach hinten verschoben werden.

Das Ziel ist eine Entlastung bei Systemen, für die harmonisierte Standards oder Umsetzungsleitlinien noch nicht ausreichend vorliegen. Praktisch bedeutet dies jedoch, dass der Rechtsrahmen zwar später greift, aber nicht automatisch einfacher wird.

2. AI Literacy

Gegenstand des Entwurfs zum Digitalen Omnibus ist zudem die Pflicht zur Sicherstellung von AI Literacy beziehungsweise KI-Kompetenz. Teilweise wird eine Abschwächung oder Verlagerung hin zu Förder- und Unterstützungsmaßnahmen statt einer harten Unternehmenspflicht vorgeschlagen.

Regulatorisch ist dies bedeutsam, weil KI-Kompetenz als Scharnier zwischen Technik, Governance und Compliance fungiert. Fällt diese Pflicht weg oder wird sie aufgeweicht, verlagert sich die Verantwortung stärker auf freiwillige interne Organisationsentscheidungen.

3. Sektorale Ausnahmen

Besonders umstritten sind Vorschläge, bestimmte Produktsektoren aus der unmittelbaren Anwendung der KI-Verordnung herauszunehmen oder stärker in sektorale Regelungen zu verschieben. Kritiker befürchten, dass dadurch der einheitliche, risikobasierte Ansatz der Verordnung ausgehöhlt wird.

Verschiedene Fachbeiträge weisen darauf hin, dass dies zu Fragmentierung führen könnte, weil für einzelne Branchen dann unterschiedliche Rechtslogiken nebeneinander gelten würden. Damit wäre das Ziel der Vereinfachung zumindest teilweise verfehlt.

4. Bias-Checks und besondere Daten

Ein zentraler Punkt ist außerdem die Nutzung besonderer Kategorien personenbezogener Daten zur Bias-Erkennung und -Korrektur. Hier geht die Kommission in Richtung einer ausdrücklich geregelten Ausnahme, um diskriminierungsarme KI-Entwicklung zu ermöglichen.

Die Aufsichtsbehörden halten auch diesen Ansatz nur unter strengen Bedingungen für akzeptabel. Sie verlangen insbesondere die Gewährleistung von Verhältnismäßigkeit, Sicherheit, Zweckbindung und Löschung nach Abschluss des Zwecks.

VII. Aufsichtsrechtliche Bewertung

Die EDPB/EDPS-„Joint Opinion“ ist die relevanteste Gegenstimme zum Entwurf. Sie begrüßt einzelne Vereinfachungen, lehnt jedoch insbesondere die Umgestaltung des Personenbegriffs und die Auslagerung zentraler Abgrenzungsentscheidungen in Durchführungsrechtsakte ab.

Aus rechtsstaatlicher Perspektive ist das bedeutsam, weil Datenschutzrecht in der Union nicht nur Verwaltungsrecht, sondern sekundärrechtlich kodifiziertes Grundrechtsrecht ist. Eine Reform darf daher nicht bloß Effizienzgewinne anstreben, sondern muss die Schutzintensität und die dogmatische Stabilität des Systems mitdenken und sicherstellen.

VIII. Praktische Folgen für Unternehmen

Unternehmen müssen sich darauf einstellen, dass der Omnibus nicht automatisch zu weniger rechtlichen Anforderungen im Sinne der Compliance führt. Vielmehr verschiebt sich der Schwerpunkt auf präzisere Datenklassifizierung, dokumentierte Identifizierbarkeitsprüfungen und robustere Governance für KI-Trainingsprozesse.

Für datenverarbeitende Unternehmen ist besonders relevant, wer im konkreten Workflow über Re-Identifizierungs- oder Zugriffsmöglichkeiten verfügt. Je stärker der Entwurf umgesetzt wird, desto wichtiger wird die differenzierte Betrachtung einzelner Verarbeitungseinheiten, Kontexte und Empfänger.

1. KI-Training

Für das Training von KI-Systemen dürfte die Legitimation über berechtigte Interessen oder spezifische Ausnahmen größere Bedeutung gewinnen. Das nimmt den Unternehmen aber nicht die Pflicht, den Einsatz datenminimierend, sicher und transparent zu gestalten.

2. Compliance-Strukturen

Sollte die KI-Regulierung stärker sektoralisiert werden, müssten Produkt-, Rechts- und Compliance-Teams innerhalb von Konzernen, Unternehmensverbänden oder Großunternehmen enger zusammenarbeiten. Dann entstünde nicht weniger, sondern tendenziell mehr Abstimmungsaufwand zwischen horizontalem KI-Recht und sektoralen Spezialregimen.

IX. Offene Rechtsfragen

Mehrere Rechtsfragen sind gegenwärtig noch offen. Dazu gehören die genaue Reichweite des neuen Personenbegriffs, die zukünftige Definition und Bewertung pseudonymisierter Daten, die Ausgestaltung der Sonderregeln für KI-Training sowie die Frage, wie weit sektorale Ausnahmen überhaupt gehen dürfen.

Hinzu kommt die institutionelle Frage, wie viel Regelungskompetenz die Europäische Kommission über Durchführungsakte erhalten soll. Gerade dort, wo Grundrechtsdogmatik betroffen ist, dürfte das Europäische Parlament als Legislative der EU einer weitreichenden Delegation kritisch gegenüberstehen.

X. Bewertung

Der Digital-Omnibus ist ein Projekt der Neujustierung, nicht bloß der bürokratischen Entlastung. Er könnte einzelne praktische Probleme lösen, birgt aber zugleich das Risiko, den Schutzstandard der DS-GVO und die Einheitlichkeit der KI-Verordnung zu schwächen.

Rechtswissenschaftlich lässt sich das Vorhaben daher als Balanceakt zwischen Effizienz, Wettbewerbsfähigkeit und Grundrechtsschutz beschreiben. Ob daraus am Ende ein kohärenteres digitales Regelwerk oder ein noch komplexeres Geflecht wird, bleibt vorerst abzuwarten und hängt maßgeblich von den laufenden Verhandlungen ab.

XI. Fazit

Der EU Digital-Omnibus zeigt, dass die europäische Digitalregulierung in eine Phase der Korrektur und Feinabstimmung eingetreten ist. Besonders die Diskussion um personenbezogene Daten und sektorale KI-Ausnahmen macht deutlich, dass Vereinfachung im Digitalrecht nicht mit Deregulierung verwechselt werden darf.

Für die Einordnung dieses Vorhabens ist es daher wichtig, den Omnibus als rechtspolitisches und dogmatisches Spannungsfeld zu behandeln: zwischen Harmonisierung und Fragmentierung, zwischen Flexibilität und Rechtssicherheit sowie zwischen Innovationsförderung und Grundrechtsschutz.

Seminartipps zum Arbeitspapier

Datenschutz Aktuell

Die Themen dieses Seminars werden stets topaktuell zusammengestellt, mit Fokus auf die wichtigsten Entwicklungen im Datenschutzrecht und deren praktischer Umsetzung. Berücksichtigt werden dabei neue Urteile, Gesetzesinitiativen, Aufsichtsbehördenpositionen sowie aktuelle Trends aus Unternehmen und Verwaltung.

- Gesetzgebung Europa und national
- Praxisrelevante Gerichtsentscheidungen
- Wichtige Veröffentlichungen

Die konkreten Schwerpunkte werden etwa sechs Wochen vor Seminarbeginn bekannt gegeben. Lassen Sie sich gerne auf unsere Vormerkliste setzen. Sie werden dann automatisch per E-Mail informiert, sobald die finalen Inhalte und Referierenden feststehen.

Weitere Infos finden Sie [hier](#).



Igor.nazlo | Sikov | plysulkvv - stock.adobe.com

Datenschutz und Künstliche Intelligenz

Künstliche Intelligenz und Datenschutz: Rechtssicherer Einsatz mit der KI-Verordnung

Der Begriff „Künstliche Intelligenz“ ist momentan in aller Munde. Es wird die nächste Stufe der wirtschaftlichen Transformation beschworen und es findet eine enorme Ausrichtung von finanziellen Mitteln auf die weitere Entwicklung und den Einsatz von künstlicher Intelligenz statt. Viele (auch kleinere und mittlere) Unternehmen stellen sich momentan – zu Recht – die Frage, ob diese schnell auf dieses Thema setzen sollten um nicht ins Hintertreffen zu geraten.

Damit ist auch der Datenschutz gefordert, diese hochkomplexe Technologie zu begleiten und die Risiken für die Betroffenen handhabbar zu halten. Zusätzlich kommt mit der KI-Verordnung, die am 01. August 2024 in Kraft getreten ist und deren Übergangsfristen schrittweise bis 2026 ablaufen eine weitere Regulierung für diese Art der Technologie.

Weitere Infos finden Sie [hier](#).



Smile Studio AP - stock.adobe.com



DataAgenda

ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext

ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.



Autoren

Prof. Dr. Rolf Schwartmann

Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.



Dr. Tobias Jacquemain, LL.M. (GDD e.V.)

Promotion zum Schadensersatz für Datenschutzverstöße nach Art. 82 DS-GVO und Lehrbeauftragter an der Universität zu Köln, an der Technischen Hochschule (TH) Köln sowie an der TH Georg Agricola in Bochum.

