BÜNDNIS F5

AlgorithmWatch
Gesellschaft für Freiheitsrechte
Open Knowledge Foundation
Reporter ohne Grenzen
Wikimedia Deutschland

info@buendnis-f5.de

Zweite Kommentierung Digitales Omnibuspaket der EU Kommission

Übersicht

Der Digitale Omnibus verfolgt laut der Europäischen Kommission das Ziel, bestehende digitale Regelwerke zu vereinfachen und ihre Anwendung zu harmonisieren. Die vorgeschlagenen Änderungen an der DSGVO, KI-VO, und den Datenrechtsakten erreichen dieses Ziel jedoch nur vereinzelt. In vielen Punkten bringt die Kommission umfassende Änderungsvorschläge ein, die auch grundrechtliche Schutzstandards betreffen.

In dieser Kommentierung betrachten wir 14 wichtige Punkte der Gesetzespakete. Das Dokument ist nicht als vollständige Kommentierung aller Vorschläge gedacht, sondern fasst unsere Einschätzungen und Analysen zu zentralen Aspekten zusammen. Jede Sektion umfasst zudem Änderungsvorschläge.

Trotz der Tiefe der vorgeschlagenen Änderungen und ihren Auswirkungen auf den Schutz der Grundrechte beinhaltet das Omnibus-Verfahren keine Gesetzesfolgenabschätzung und soll im beschleunigten Verfahren beschlossen werden. Die hier angemerkten Punkte, sowie weitere Kommentierungen insbesondere aus zivilgesellschaftlichen (und wissenschaftlichen) Kreisen, können eine umfassende Folgenabschätzung zwar nicht ersetzen, sollten jedoch unbedingt im Verfahren berücksichtigt werden.

Zu diesen und weiteren Themen stehen wir ausdrücklich für vertiefende Gespräche und einen konstruktiven Austausch zur Verfügung. Wir halten es für notwendig, die Reform der Digitalen Rechtsakte in einem breiten, transparenten und evidenzbasierten Dialog weiterzuentwickeln.

BÜNDNIS F5

AlgorithmWatch
Gesellschaft für Freiheitsrechte
Open Knowledge Foundation
Reporter ohne Grenzen
Wikimedia Deutschland

info@buendnis-f5.de

Unsere Forderungen im Überblick

BÜNDNIS F5

AlgorithmWatch
Gesellschaft für Freiheitsrechte
Open Knowledge Foundation
Reporter ohne Grenzen
Wikimedia Deutschland

info@buendnis-f5.de

Änderungen an der DSGVO

1. Objektiven Personenbezug erhalten und rechtliche Schlupflöcher verhindern.

Relevante Artikel: Art. 4 Nr. 1 DSGVO-E.

Worum es geht: Die vorgeschlagenen Änderungen zur Definition des Personenbezugs im Digital Omnibus sind eine grundlegende Abkehr vom bisherigen objektiven Schutzstandard. Durch die Einführung eines subjektiven Maßstabs soll künftig maßgeblich sein, ob eine Organisation selbst davon ausgeht, mit den ihnen zur Verfügung stehenden Mitteln eine Person identifizieren zu können. Die bloße Möglichkeit einer Identifizierung durch andere Stellen bleibt außer Betracht. Damit würde der Anwendungsbereich der DSGVO von der internen Einschätzung der Verantwortlichen abhängig gemacht. Diese Verschiebung ermöglicht es Unternehmen, Daten als nicht personenbezogen einzuordnen, obwohl sie sich faktisch auf identifizierbare Personen beziehen. Darüber hinaus kann dasselbe Datum je nach verarbeitender Stelle unterschiedlich eingestuft werden, was insbesondere innerhalb von Liefer- und Verarbeitungsketten zu einer Fragmentierung des Datenschutzrechts führt. Der Datenschutz verliert dadurch seine einheitliche und verlässliche Schutzfunktion.

Der Entwurf stützt sich auf eine selektive Auslegung einzelner Urteile und blendet andere einschlägige Entscheidungen aus. Insgesamt geht die geplante Regelung über die Rechtsprechung hinaus und senkt das bisherige Schutzniveau ab. Dies birgt erhebliche verfassungs- und unionsrechtliche Risiken. Wir sehen in der beabsichtigten Ausgestaltung einen Konflikt mit Art. 8 der EU-Grundrechtecharta und der bisherigen Rechtsprechung des EuGH. Die Grundrechtecharta knüpft an eine weite Definition personenbezogener Daten an, die auch die Möglichkeit der Identifizierung durch Dritte einbezieht.

Warum das wichtig ist: Die vorgeschlagene Änderung wird zu fundamentalen und absehbaren Durchsetzungsdefiziten führen und den Kern der DSGVO unterminieren. Aufsichtsbehörden und betroffene Personen verfügen regelmäßig nicht über die notwendigen Informationen, um zu überprüfen, welche technischen und organisatorischen Mittel einem Unternehmen tatsächlich zur Identifizierung zur Verfügung stehen. Dadurch entsteht ein strukturelles Kontrollproblem. Ohne Auskunftsanspruch kann nicht geprüft werden, ob diese Einordnung zutreffend ist. Die praktische Durchsetzung der DSGVO würde dadurch erheblich erschwert. Ob Daten personenbezogen sind, wird faktisch kaum überprüfbar. Dies verstärkt bestehende Vollzugsdefizite und erschwert die Rechtsdurchsetzung erheblich.

Zugleich wird mit der Formulierung „mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel“ eine subjektivierende Bewertung eingeführt, die stark abhängig von der individuellen Einschätzung und organisatorischen Strukturen des jeweiligen Verantwortlichen ist. Damit ist nicht mehr allein die objektive Identifizierbarkeit maßgeblich und der Anwendungsbereich der DSGVO wird in erheblichem Umfang in die Verantwortung der datenverarbeitenden Stellen verlagert. Dies führt zu Rechtsunsicherheiten bei Betroffenen und struktureller Schwächung ihrer Rechte.

Was wir empfehlen:

- Verzicht auf die vorgeschlagene vermeintliche Klarstellung in Art. 4 Nr. 1 DSGVO-E, da sie keinen substanziellen Mehrwert bietet, aber neue Risiken schafft.
- Beibehaltung des objektiven Maßstabs aus Erwägungsgrund 26 DSGVO („Verantwortlichen oder einer anderen Person“).
- Klarstellung in den Erwägungsgründen, dass der Personenbezug nicht allein von der Selbsteinschätzung des Verantwortlichen abhängt.
- Stärkung der Aufsichtsbefugnisse zur Überprüfung der tatsächlichen Identifizierbarkeit.

2. Schutzstandards für pseudonymisierte Daten nicht administrativ absenken.

Relevante Artikel: Art. 41a, Erwägungsgrund 27 DSGVO-E.

Worum es geht: Der Erwägungsgrund 27 DSGVO-E schlägt vor, dass pseudonymisierte Daten nicht für jede Stelle automatisch personenbezogen sein sollen. Dies entspricht grundsätzlich der bisherigen Systematik, nach der Pseudonymisierung keine eigenständige Datenkategorie begründet, sondern ein Instrument der Risikominderung darstellt.

Problematisch ist jedoch die Einführung von Art. 41a DSGVO-E. Dieser ermächtigt die Kommission, per Durchführungsrechtsakt festzulegen, wann pseudonymisierte Daten keinen Personenbezug mehr aufweisen. Damit erhält die Kommission, ohne Mitsprache des Rates und des Parlamentes, erheblichen Einfluss auf die Bestimmung des Schutzbereichs der DSGVO.

Zudem vermischt der Entwurf die Konzepte der Pseudonymisierung und der Anonymisierung. Die binäre Entscheidung über das Vorliegen eines Personenbezugs wird mit technischen Kriterien verknüpft, obwohl sie kontextabhängig ist. Dies gefährdet die Systematik der DSGVO und führt zu zusätzlicher Rechtsunsicherheit.

Warum das wichtig ist: Pseudonymisierung ist ein zentrales Instrument zur Reduzierung der Risiken bei der Datenverarbeitung. Wenn sie faktisch zu einer Herausnahme aus dem Anwendungsbereich der DSGVO führt, gehen wesentliche Schutzmechanismen und Betroffenenrechte verloren.

Zugleich verschiebt Art. 41a DSGVO-E Auslegungskompetenzen von unabhängigen Aufsichtsbehörden zur Europäischen Kommission. Dies steht in Spannung zu Art. 8 Abs. 3 GRCh und kann die institutionelle Balance im Datenschutzrecht beeinträchtigen.

Was wir empfehlen:

- Streichung von Art. 41a DSGVO-E in seiner derzeitigen Form.
- Klarstellung, dass pseudonymisierte Daten für Stellen mit Zugriff auf relevantes Zusatzwissen, insbesondere wenn dies die Identifikation ermöglicht, stets personenbezogen bleiben.
- Beschränkung möglicher Durchführungsrechtsakte auf technische Leitlinien zur Risikominderung. Keine grundsätzliche Verschiebung des Anwendungsbereiches.

BÜNDNIS F5

AlgorithmWatch
Gesellschaft für Freiheitsrechte
Open Knowledge Foundation
Reporter ohne Grenzen
Wikimedia Deutschland

info@buendnis-f5.de

3. Forschungsprivileg klar begrenzen und Missbrauch verhindern.

Relevante Artikel: Art. 4 Nr. 38 DSGVO-E.

Worum es geht: Die Kommission schlägt vor, den Begriff der wissenschaftlichen Forschung ausdrücklich auf privatwirtschaftliche und kommerzielle Forschung auszuweiten. Damit sollen nicht nur Universitäten und öffentliche Forschungseinrichtungen, sondern auch Unternehmen und private Labore von datenschutzrechtlichen Privilegierungen profitieren.

Diese Ausweitung zielt offenbar darauf ab, Innovationshemmnisse abzubauen und datenintensive Forschung zu erleichtern, wobei sie insbesondere im Bereich von KI, Medizin und Verhaltensforschung von besonderer Relevanz sein dürfte. Gleichzeitig verzichtet der Entwurf weitgehend auf materielle Kriterien, die eine Abgrenzung zwischen genuiner Forschung und rein kommerzieller Datenverwertung erlauben würden.

Das zentrale Problem liegt in der fehlenden Konturierung des Forschungsbegriffs. Ohne verbindliche inhaltliche Maßstäbe droht, dass nahezu jede datenbasierte Produktentwicklung oder Marktanalyse als „Forschung“ deklariert werden kann. Dadurch wird das Privileg potenziell entgrenzt und verliert seinen Ausnahmecharakter.

Warum das wichtig ist: Der Forschungsbegriff bildet die Grundlage für weitreichende Abweichungen von zentralen Datenschutzprinzipien. Je weiter er gefasst wird, desto größer wird der Bereich, in dem Grundrechte eingeschränkt werden dürfen. Der Fall Cambridge Analytica zeigt exemplarisch, dass eine Datenverarbeitung, die zunächst als „wissenschaftliche Forschung“ deklariert wird, später für andere, grundrechtsgefährdende Zwecke genutzt werden kann.

Die vorgeschlagene Definition weitet den Forschungsbegriff in einer Weise aus, die mit dem Ausnahmecharakter datenschutzrechtlicher Privilegierungen nicht vereinbar ist. Insbesondere die Bezugnahme auf „jede Forschungstätigkeit, die auch Innovationen [...] unterstützen kann“, auf „neuartige Anwendungen vorhandener Erkenntnisse“ sowie auf Tätigkeiten, die „zum Wohlergehen der Gesellschaft beitragen“, eröffnet einen sehr weiten

Interpretationsspielraum und ermöglicht eine Privilegierung rein kommerzieller und im Kern nicht forschender Datenverarbeitungen.

Eine unklare Definition begünstigt strategische Umgehungen der DSGVO. Unternehmen könnten reguläre Profilbildung, Verhaltensanalyse oder Produktoptimierung unter dem Label „Forschung" betreiben, ohne den Schutzstandard einhalten zu müssen. Dies gefährdet das Vertrauen in datenschutzrechtliche Ausnahmeregelungen insgesamt.

Was wir empfehlen:

- Den Verzicht auf Einführung des Art. 4 Nr. 38 DSGVO-E in der vorliegenden Form oder grundsätzliche Änderungen.
- Sollte sich im weiteren Gesetzgebungsverfahren zeigen, dass eine Neuregelung erforderlich ist, sollte der Definitionsrahmen deutlich enger und hinreichend bestimmt gefasst werden. Rein marktorientierte oder primär wirtschaftliche Tätigkeiten dürfen nicht unter das Forschungsprivileg fallen.
- Maßgeblich sollten insbesondere ein nachvollziehbarer Erkenntnisgewinn, methodische Transparenz und ein wissenschaftlicher Mehrwert sein, insbesondere durch eine Pflicht zur Veröffentlichung und Dokumentation der Forschungsergebnisse.
- Darüber hinaus braucht es im Gesetz klarstellende Auslegungshilfen für die Aufsichtsbehörden (ggf. in Form von Erwägungsgründen).
- Ohne eine solche Präzisierung sollte von der Einführung der neuen Vorschrift abgesehen und Art. 4 Nr. 38 DSGVO-E gestrichen werden.

4. Auskunftsrechte vor missbräuchlicher Einschränkung schützen.

Relevante Artikel: Art. 12 Abs. 5 DSGVO-E.

Worum es geht: Der Vorschlag erweitert den bisherigen Ablehnungsgrund für Auskunftsersuche um den Tatbestand des „Missbrauchs". Künftig sollen Anfragen auch dann als exzessiv gelten, wenn sie aus anderen Motiven als allein aus datenschutzbezogenen Gründen gestellt werden. Gleichzeitig wird die Beweislast für

Verantwortliche abgesenkt, indem bereits „hinreichende Gründe für die Annahme“ ausreichen sollen, um Anträge als exzessiv zu bewerten.

Damit wird erstmals eine Zweckbindung für die Ausübung von Betroffenenrechten eingeführt, was zu einer Verschiebung der Beweislast zulasten der Betroffenen führt. Die betroffene Person soll faktisch darlegen müssen, dass ihr Anliegen ausschließlich datenschutzbezogen motiviert ist. Dies widerspricht dem bisherigen Verständnis des Auskunftsrechts als eigenständigem, motivationsunabhängigem Grundrecht.

Praktisch eröffnet die Regelung einen erheblichen Ermessensspielraum für Verantwortliche. Diese müssten die Motive der anfragenden Person bewerten, obwohl solche Motive regelmäßig nicht objektiv feststellbar sind. Dies schafft ein strukturelles Ungleichgewicht zulasten der Betroffenen und erhöht die Gefahr pauschaler Ablehnungen.

Warum das wichtig ist: Das Auskunftsrecht ist in Art. 8 Abs. 2 Satz 2 der EU-Grundrechtecharta ausdrücklich verankert, unterliegt keiner Zweckbindung und gehört zu den Kerngewährleistungen des europäischen Datenschutzrechts. Es ermöglicht Betroffenen, informationelle Machtasymmetrien gegenüber Unternehmen und Behörden auszugleichen.

In der Praxis dient das Auskunftsrecht häufig der Vorbereitung arbeits-, verbraucher- oder schadensersatzrechtlicher Ansprüche, der Aufdeckung von Diskriminierung oder der journalistischen und wissenschaftlichen Kontrolle. Eine Einschränkung auf „datenschutzbezogene“ Zwecke würde diese Funktionen erheblich schwächen.

Zudem besteht kein empirisch belegtes strukturelles Missbrauchsproblem. Bereits heute erlaubt Art. 12 Abs. 5 DSGVO die Zurückweisung offensichtlich unbegründeter oder exzessiver Anträge. Die vorgeschlagene Erweiterung ist daher weder notwendig noch verhältnismäßig.

Was wir empfehlen:

- Der vorgeschlagene Missbrauchstatbestand sollte vollständig gestrichen werden. Die bestehende Regelung des Art. 12 Abs. 5 DSGVO bietet bereits ein ausreichendes Instrumentarium zur Abwehr missbräuchlicher Anfragen.

- Sollte politisch dennoch Handlungsbedarf gesehen werden, kommt allenfalls eine eng begrenzte Klarstellung in Betracht, die ausdrücklich nur Fälle gezielter Schikane oder Erpressung erfasst. Diese müsste an objektive Kriterien anknüpfen und die volle Beweislast beim Verantwortlichen belassen.
- Darüber hinaus sollte klargestellt werden, dass die Ausübung von Betroffenenrechten grundsätzlich motivationsunabhängig ist und nicht von der Offenlegung persönlicher Beweggründe abhängig gemacht werden darf.

5. Pragmatische Erleichterungen bei Informationspflichten einführen und verantwortungsvoll ausgestalten.

Relevante Artikel: Art. 13 Abs. 4, Erwägungsgrund 36 DSGVO-E.

Worum es geht: Die Kommission schlägt vor, die Informationspflicht bei direkter Datenerhebung in bestimmten alltäglichen Konstellationen zu lockern. Erfasst werden sollen insbesondere einfache Vertrags- oder Vereinsverhältnisse mit geringer Datenintensität.

Die Regelung knüpft an mehrere kumulative Voraussetzungen an: eine klar umschriebene Beziehung, geringe Datenintensität, kein Drittlandtransfer, keine automatisierte Entscheidung und kein hohes Risiko. Zudem müssen „hinreichende Gründe" bestehen, dass die betroffene Person informiert ist.

Es ist zu prüfen, ob die Vielzahl unbestimmter Rechtsbegriffe eine verlässliche Anwendung erschwert. Begriffe wie „klaren und begrenzten Beziehung" oder „nicht datenintensive Tätigkeit" sind auslegungsbedürftig und schaffen Unsicherheiten. Gleichzeitig handelt es sich um pragmatische Erleichterungen, die im Kern dazu beitragen, die DSGVO praktikabler auszugestalten.

Warum das wichtig ist: Die vorgeschlagene Anpassung der Informationspflichten trägt dem Umstand Rechnung, dass die bisherigen Vorgaben der DSGVO in alltäglichen, wenig datenintensiven Konstellationen häufig mit erhöhtem administrativen Aufwand verbunden

sein können. Gerade kleinere Organisationen, Vereine oder lokale Dienstleister sehen sich regelmäßig mit komplizierten Informationspflichten konfrontiert. Eine differenzierte Ausgestaltung kann hier zu mehr Praktikabilität und Akzeptanz des Datenschutzrechts beitragen.

Durch die Fokussierung auf klar begrenzte Beziehungskonstellationen und geringes Risikopotenzial eröffnet die Regelung die Möglichkeit, Datenschutz stärker risikobasiert auszugestalten. Dies entspricht dem Grundgedanken der DSGVO, Schutzmechanismen dort besonders zu konzentrieren, wo tatsächlich erhebliche Grundrechtsgefährdungen bestehen. Gleichzeitig werden Ressourcen von Verantwortlichen und Aufsichtsbehörden frei, die gezielter für komplexe und besonders eingriffsintensive Verarbeitungsvorgänge eingesetzt werden können.

Zudem kann die Regelung dazu beitragen, die tatsächliche Wirksamkeit von Transparenz zu erhöhen. Standardisierte, formelhafte Datenschutzhinweise werden von Betroffenen häufig nicht gelesen oder verstanden. Eine stärkere Konzentration auf wesentliche Informationen in relevanten Konstellationen bietet die Chance, Transparenz inhaltlich zu verbessern, statt sie lediglich formal zu erfüllen. Voraussetzung hierfür ist jedoch, dass die Ausnahmen klar begrenzt bleiben und durch effektive Kontrollmechanismen flankiert werden.

Was wir empfehlen:

- Der Vorschlag ist zu begrüßen.
- Die Regelung könnte durch eine Auskunftspflicht auf Anfrage in praktikablem Umfang ergänzt werden, um weiterhin die Klärung von Unklarheiten zu ermöglichen. Es erscheint fraglich, ob der Zugang zu diesen Informationen gesetzlich vollständig ausgeschlossen werden sollte.

6. Klare Regeln für KI-Datenverarbeitung statt pauschaler Öffnungsklauseln.

Relevante Artikel: Art. 88c, Erwägungsgrund 27f. DSGVO-E.

Worum es geht: Art. 88c DSGVO-E verzichtet weitgehend auf verbindliche, risikobasierte Schutzstandards und differenziert nicht systematisch zwischen besonders eingriffsintensiven und weniger sensiblen Einsatzkontexten. Statt konkrete Anforderungen an Transparenz, Fairness, Zweckbindung oder menschliche Kontrolle festzulegen, beschränkt sich die Norm auf abstrakte Verweise auf Datenminimierung und organisatorische Maßnahmen. Dadurch entsteht die Gefahr, dass insbesondere in Bereichen mit hohem Missbrauchs- und Diskriminierungspotenzial kein verlässliches Schutzniveau gewährleistet wird.

Vor diesem Hintergrund ist es zunächst nachvollziehbar, dass der Entwurf versucht, die Position betroffener Personen durch ein voraussetzungsloses Widerspruchsrecht zu stärken. Dieses Instrument soll sicherstellen, dass Individuen auch bei komplexen und intransparenten KI-Verarbeitungen eine effektive Einflussmöglichkeit behalten. In der Praxis stößt dieses Konzept jedoch an erhebliche Grenzen, insbesondere bei großskaligen Trainings- und Entwicklungsprozessen. Die nachträgliche Identifikation und Entfernung einzelner Datensätze ist häufig technisch kaum umsetzbar und kann bestehende Systeme strukturell destabilisieren.

Hierdurch entsteht ein Spannungsverhältnis zwischen berechtigtem Grundrechtsschutz und praktischer Umsetzbarkeit. Das Widerspruchsrecht ist Ausdruck eines hohen Schutzanspruchs, entfaltet aber in seiner voraussetzungslosen Ausgestaltung eine erhebliche Rechtsunsicherheit für Entwickler*innen und Betreiber. Anstelle klarer, vorhersehbarer Anforderungen entstehen schwer kalkulierbare Risiken, die weder dem Schutz der Betroffenen noch der Rechtssicherheit der Verantwortlichen dienen.

Insgesamt führt diese Konstruktion dazu, dass Art. 88c DSGVO-E den Schutz personenbezogener Daten nicht systematisch stärkt, sondern fragmentarisch und widersprüchlich ausgestaltet. Wesentliche Schutzdefizite bleiben bestehen, während punktuelle Verschärfungen neue praktische Probleme schaffen. Die Regelung verfehlt somit ihr Ziel, einen ausgewogenen und verlässlichen Rechtsrahmen für KI zu etablieren. Vor diesem Hintergrund sollte Art. 88c DSGVO-E in seiner derzeitigen Form nicht beibehalten, sondern durch eine kohärente, risikobasierte und grundrechtsorientierte Regelung ersetzt werden.

Warum das wichtig ist: Die Regelung betrifft einen zentralen Zukunftsbereich der digitalen Gesellschaft. KI-Systeme werden zunehmend in sensiblen Bereichen eingesetzt, etwa bei Personalentscheidungen, Kreditwürdigkeitsprüfungen, Gesundheitsanwendungen oder im Sicherheitsbereich. Die Art und Weise, wie Trainingsdaten erhoben, verarbeitet und ausgewertet werden, beeinflusst unmittelbar die Grundrechte der Betroffenen.

Unklare oder unzureichende Regelungen führen zudem zu strukturellen Risiken. Große Plattform- und KI-Unternehmen verfügen über die Ressourcen, um rechtliche Unsicherheiten strategisch zu nutzen oder undurchsichtige Compliance-Strukturen aufzubauen. Kleine und mittlere Unternehmen geraten hingegen unter Druck, weil sie sich entweder aus Innovationsfeldern zurückziehen oder erhebliche Rechtsrisiken eingehen müssen. Damit wird der Wettbewerb verzerrt und das Ziel eines fairen digitalen Binnenmarkts gefährdet.

Was wir empfehlen:

- Streichen des neuen 88c DSGVO-E.

7. Schutz sensibler Daten auch im KI-Kontext konsequent sichern.

Relevante Artikel: Art. 9 Abs. 2 k und 5 DSGVO-E.

Worum es geht: Art. 9 DSGVO enthält bislang ein grundsätzliches Verarbeitungsverbot für besonders sensible Daten, etwa Gesundheitsdaten, biometrische Daten, politische Meinungen oder religiöse Überzeugungen. Dieses Verbot darf nur unter eng begrenzten Ausnahmen durchbrochen werden. Die neuen Absätze sollen nun eine spezifische Öffnung für KI-Zwecke schaffen.

Der Entwurf versucht, zwei widersprüchliche Ziele zu verbinden: Einerseits wird die Verarbeitung sensibler Daten für KI-Systeme ausdrücklich erlaubt, andererseits soll sie „soweit wie möglich vermieden“ werden. Diese Doppelstruktur bleibt inhaltlich unklar. Es wird nicht definiert, wann eine Vermeidung als ausreichend gilt und welche Alternativen geprüft werden müssen.

Besonders problematisch ist zudem, dass die Regelung nicht hinreichend berücksichtigt, dass viele sensible Merkmale heute nicht direkt erhoben, sondern algorithmisch abgeleitet werden. Politische Einstellungen, Gesundheitszustände oder sexuelle Orientierung lassen sich häufig aus scheinbar neutralen Verhaltensdaten rekonstruieren. Der Entwurf trägt dieser Realität nur unzureichend Rechnung.

Warum das wichtig ist: Besondere Kategorien personenbezogener Daten stehen in einem engen Zusammenhang mit Diskriminierungsrisiken. Historisch und gegenwärtig werden solche Daten zu sozialer Ausgrenzung, Überwachung und Stigmatisierung genutzt. KI-Systeme verstärken diese Risiken und können gesellschaftliche Diskriminierungsmuster reproduzieren indem sie Muster automatisiert erkennen und skalieren.

Wenn der Schutz sensibler Daten im Kontext von KI abgeschwächt wird, droht eine systematische Verschiebung der Schutzstandards. Diskriminierung verlagert sich zunehmend auf intransparente statistische und probabilistische Verfahren, die für Betroffene kaum nachvollziehbar sind. Die rechtliche Kontrolle solcher Prozesse ist daher besonders anspruchsvoll und zugleich unverzichtbar.

Was wir empfehlen:

- Rücknahme der entsprechenden Änderungsvorschläge in Art. 9

8. Datenschutz-Folgenabschätzungen harmonisieren.

Relevante Artikel: Art. 35 Abs. 4, 5 und 6 DSGVO-E.

Worum es geht: Die Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO dient dazu, hohe Risiken für die Rechte und Freiheiten betroffener Personen frühzeitig zu identifizieren und zu minimieren. Nach geltendem Recht erstellen nationale Aufsichtsbehörden eigene Positiv- und Negativlisten, die festlegen, wann eine DSFA erforderlich ist. Dies hat in der Praxis zu einer Vielzahl unterschiedlicher Regelungen geführt.

Der Digital Omnibus sieht vor, diese Zuständigkeit auf europäischer Ebene zu bündeln. Künftig soll der Europäische Datenschutzausschuss (EDSA) unionsweit geltende Black- und Whitelists sowie ein einheitliches Formular und eine gemeinsame Methodik vorschlagen, die von der Kommission per Durchführungsrechtsakt verabschiedet werden. Ziel ist eine stärkere Harmonisierung und Vereinfachung.

Warum das wichtig ist: Die DSFA ist ein zentrales Instrument des präventiven Grundrechtsschutzes. Sie zwingt Verantwortliche dazu, sich frühzeitig mit möglichen negativen Folgen ihrer Datenverarbeitungen auseinanderzusetzen und Schutzmaßnahmen zu entwickeln. Eine Schwächung oder Formalisierung dieses Instruments kann potentiell dazu führen, dass Risiken nur noch schematisch geprüft werden.

Gleichzeitig ist die derzeitige Fragmentierung ein reales Problem für grenzüberschreitend tätige Organisationen. Unterschiedliche nationale Anforderungen erzeugen Rechtsunsicherheit und erhöhen den administrativen Aufwand. Eine unionsweite Harmonisierung kann daher zur besseren Durchsetzbarkeit und Akzeptanz des Datenschutzrechts beitragen, sofern sie qualitativ hochwertig ausgestaltet wird.

Was wir empfehlen:

- Die Einführung unionsweiter Black- und Whitelists sowie einer gemeinsamen Methodik sollte grundsätzlich unterstützt werden, da sie Rechtssicherheit und Kohärenz fördern kann.

9. Technisches Einwilligungsmanagement wirksam und nutzungsfreundlich gestalten.

Relevante Artikel: Art. 88b DSGVO-E.

Worum es geht: Art. 88b DSGVO-E sieht vor, dass Nutzerinnen und Nutzer ihre Datenschutzpräferenzen künftig über technische Signale, etwa innerhalb eines Browsers,

ausdrücken können. Diese Signale sollen Einwilligung, Ablehnung oder Widerspruch automatisiert an Websites übermitteln. Ziel ist es, Cookie-Banner weitgehend zu ersetzen und die sogenannte „Consent Fatigue“ zu überwinden.

Die Regelung verpflichtet Anbieter, solche maschinenlesbaren Präferenzen zu akzeptieren, und verpflichtet Browserhersteller, entsprechende Funktionen bereitzustellen. Damit wird ein langfristig diskutiertes Konzept technischer Datenschutzsignale erstmals verbindlich verankert.

Defizite bestehen jedoch in mehreren Punkten. Der Entwurf erfasst den Widerruf der Einwilligung nicht ausdrücklich. Zudem sind die Übergangsfristen sehr lang und die Standardisierung soll an externe Gremien ausgelagert werden.

Warum das wichtig ist: Ein funktionierendes technisches Einwilligungsmanagement kann die informationelle Selbstbestimmung erheblich stärken. Es ermöglicht Nutzerinnen und Nutzern, ihre Präferenzen dauerhaft und konsistent umzusetzen, ohne täglich mit unübersichtlichen Bannern konfrontiert zu werden.

Gleichzeitig verschiebt Art. 88b Machtstrukturen im digitalen Raum. Die Gestaltung der Schnittstellen bestimmt, wie wirksam Rechte ausgeübt werden können. Ohne klare Vorgaben besteht die Gefahr, dass neue Abhängigkeiten von dominanten Browseranbietern entstehen oder industriegetriebene Standards den Schutz aushöhlen.

Was wir empfehlen:

- Verpflichtung aller relevanten Plattformen: Die Pflicht zur Umsetzung darf sich nicht auf klassische Webbrowser beschränken. Auch Betriebssysteme, In-App-Browser und andere Endnutzer-Software müssen einbezogen werden.
- Kürzere Übergangsfristen: Die Fristen von 24 bzw. 48 Monaten sollten deutlich verkürzt werden, um eine zeitnahe Wirkung zu erzielen.
- Standardsetzung durch die Kommission: Die Kommission sollte Mindestanforderungen selbst per Durchführungsrechtsakt festlegen, statt die Ausgestaltung primär an Standardisierungsgremien auszulagern.
- Mindestanforderungen im Gesetzestext: Das Gesetz sollte zentrale technische und funktionale Mindeststandards enthalten, etwa zu Zweckbindung, Granularität und Transparenz der Signale.

- Privacy by Default: Bei Installation von Browsern oder Betriebssystemen sollte verpflichtend nach Datenschutzpräferenzen gefragt werden und datenschutzfreundliche Voreinstellungen gesetzlich vorgegeben werden.
- Regelung zum Widerruf: Es muss gesetzlich sichergestellt sein, dass eine erteilte Einwilligung jederzeit einfach und in gleicher Form über dieselbe Schnittstelle widerrufen werden kann.

Änderungen an der KI-Verordnung

10. Registrierungspflicht für selbst gewährte Ausnahmen von Hochrisiko-KI-Vorgaben beibehalten.

Relevante Artikel: Art. 6 Abs. 4 KI-VO-E.

Worum es geht: Der Digitale Omnibus zu KI sieht eine Streichung von Art. 6 Abs. 4 KI-Verordnung vor. Dieser Artikel beinhaltet eine Registrierungspflicht, wenn sich Anbieter selbst von Hochrisiko-Verpflichtungen ausnehmen. Sie wurde eingeführt, um diese Selbstbefreiung öffentlich nachvollziehbar zu machen.

Der administrative Aufwand (und damit das Einsparpotenzial) ist gering: Es wird von der Europäischen Kommission selbst auf nur 100 Euro pro Unternehmen beziffert, weil lediglich grundlegende Informationen wie Kontaktdaten, die Systembeschreibung und die Begründung für die Ausnahme in der EU-Datenbank vermerkt werden sollten.

Warum das wichtig ist: Die fehlende Registrierung würde eine effektive Kontrolle und Aufsicht durch Behörden und externe Dritte wie zivilgesellschaftliche Organisationen verunmöglichen und die Rechtsdurchsetzung der KI-VO-Vorgaben deutlich erschweren. Ein Überblick über die Anzahl der Ausnahmen, sowie über Unterschiede zwischen Mitgliedstaaten würde hierdurch verhindert, was die Harmonisierung im Binnenmarkt schwächt. Außerdem wird auch Unternehmen die Möglichkeit genommen, nachzuvollziehen, wenn ein Wettbewerber ein konkurrierendes Produkt anders klassifiziert als sie selbst.

Anbieter erhalten dadurch eine intransparente Möglichkeit, sich den Verpflichtungen für Hochrisiko-KI-Systeme zu entziehen. Das schafft einen gefährlichen Fehlanreiz, die

Anforderungen der KI-VO zu umgehen. Dieser Fehlanreiz wirkt zum Nachteil verantwortungsbewusster Anbieter, die vertrauenswürdige Hochrisiko-KI-Systeme entwickeln wollen.

Die Streichung der Registrierung der Selbstbefreiung birgt zudem nachgelagerte rechtliche Risiken für Anwender von KI-Systemen: Gibt ein KI-Anbieter an, dass ein KI-System nicht in den Hoch-Risiko-Bereich fällt und nimmt keine entsprechenden Sicherheitsvorkehrungen vor, können unentdeckte Risiken in der Anwendung auftreten und zu Schäden führen, für die Anwender beispielsweise unter anderen Rechtsregimen (z.B. AGG) verantwortlich gemacht werden können.

Was wir empfehlen:

- Von der Streichung des Artikel 6 Absatz 4 KI-VO muss abgesehen werden.

11. Pauschale Fristverlängerungen für Hochrisiko-KI-Vorgaben und Kennzeichnungspflichten vermeiden.

Relevante Artikel: Art. 111, Art. 50 Abs. 2 KI-VO-E.

Worum es geht: Die Umsetzungsfrist für die Anwendung von Hochrisiko-KI-Vorgaben läuft am 2. August 2026 ab. Der Digitale Omnibus zu KI sieht eine pauschale Fristverlängerung vor, die zur Folge hat, dass sämtliche Pflichten nicht bis zu diesem Fristdatum erfüllt werden müssen. Vorgaben für Hochrisiko-KI nach Artikel 6 Absatz 2 in Verbindung mit Anhang III KI-VO würden erst ab dem 2. Dezember 2027 gelten. Vorgaben für Hochrisiko-KI nach Artikel 6 Absatz 1 und Annex I KI-VO in Verbindung mit sektoral regulierten Produkten (z. B. Medizinprodukte, Kinderspielzeug) sollen nach dem Vorschlag der Europäischen Kommission sogar erst ab dem 2. August 2028 greifen. Die Kennzeichnungspflicht für generative KI-Systeme nach Artikel 50 Abs. 2 KI-VO soll nach dem Vorschlag der Europäischen Kommission erst ab dem 2. Februar 2027 gelten.

Warum das wichtig ist: Die pauschale Fristverlängerung würde auch die Kennzeichnungspflicht nach Art. 50 KI-VO umfassen. Für Betroffene und Aufsichtsbehörden würde dies bedeuten, dass sie im Zweifel nicht eindeutig nachvollziehen können, wann und inwiefern sie einem KI-basierten Prozess oder einer automatisierten Entscheidung ausgesetzt sind. Dieser Umstand würde die

Rechtsdurchsetzung massiv erschweren, beispielsweise die Verfolgung von Einsätzen verbotener Systeme, die fälschlicherweise als Hochrisiko-Systeme gekennzeichnet würden, sowie Klagewege effektiv verstellen. Ebenso wären indirekt die Rechte auf Auskunft und Erklärung davon betroffen.

Was wir empfehlen:

- Kennzeichnungspflichten und die Anwendbarkeit von Auskunft- und Erklärungsrechten sollten von den Fristverlängerungen ausgenommen werden.

12. Regulatorische Vereinfachungen für kleine und mittlere Unternehmen (KMU) nicht auf größere Unternehmen (SMCs) ausweiten.

Relevante Artikel: Art. 11 Abs. 1 UAbs. 2, Art. 99 Abs. 6 KI-VO-E.

Worum es geht: Der Digitale Omnibus zu KI sieht vor, dass bestehende regulatorische Privilegien der KI-Verordnung von KMU in Bezug auf die technische Dokumentation und die Einrichtung eines Qualitätsmanagementsystems auf sogenannte kleine Midcaps (SMCs) ausgeweitet werden. Darüber hinaus sollen die bestehenden regulatorischen Privilegien von KMUs bei der Berechnung von Sanktionen ebenso auf SMCs ausgeweitet werden.

Warum das wichtig ist: Wenn man genauer betrachtet, wie die Europäische Kommission "kleine Mid-Cap-Unternehmen" definiert, wird erkennbar, dass die Bezeichnung geradezu irreführend ist, denn darunter fallen auch mittelgroße Unternehmen mit bis zu 749 Mitarbeiter*innen und einem Jahresumsatz von bis zu € 150 Millionen. Auch solche Unternehmen können KI-Systeme vertreiben, die Auswirkungen auf eine signifikante Anzahl von Menschen haben können.[1] Das Risiko von KI-Systemen kann daher nicht sinnvoll mit der Größe eines Unternehmens in Zusammenhang gesetzt werden. Die KI-Verordnung folgt diesem Umstand entsprechend einer Logik, die Risiken an Technologie und Einsatzkontext knüpft, nicht an Unternehmensgröße.

[1] Beispielsweise wird das Freiburger Unternehmen *Black Forest Labs* seitens der Bundesregierung als eines der erfolgversprechendsten Unternehmen in Deutschland bezeichnet. In den letzten zwei Jahren schloss es u.a. Verträge mit Branchengrößen wie Meta, Adobe und Canva ab – und dies bei einem Jahresumsatz von knapp € 100 Millionen im Jahr 2025 und knapp 50 Mitarbeiter*innen.

Die bestehenden Privilegien von KMU werden mit fehlenden Ressourcen zur Umsetzung der Compliance-Anforderungen begründet. Dieser Umstand ist bei SMCs nicht gegeben und steht nicht im Verhältnis zur potenziell einhergehenden Schwächung des Schutzes von Gesundheit, Sicherheit und Grundrechten von einer signifikanten Anzahl an Menschen.

Was wir empfehlen:

- Die vorgesehene Ausweitung regulatorischer Vereinfachungen auf "kleine Mid-Cap-Unternehmen" sollte zurückgenommen werden.

13. Befugnisse der Grundrechtsschutz-Stellen nicht einschränken.

Relevante Artikel: Art. 77 Abs. 1 KI-VO-E.

Worum es geht: Der Digitale Omnibus zu KI sieht vor, dass Stellen, die Grundrechte im Rahmen der KI-Verordnung schützen (Artikel-77-Stellen, dazu zählen u. a. die Datenschutzbehörden und die Antidiskriminierungsstelle des Bundes) die Dokumentation zu Hochrisiko-KI-Systemen nicht mehr direkt anfragen können. Diese Anfragen sollen künftig nur noch indirekt über die Marktüberwachungsbehörden (MSAs) möglich sein.

Warum das wichtig ist: Diese Änderung bedeutet eine zusätzliche Belastung für Artikel-77-Stellen und die Marktüberwachungsbehörden und kann die Wirksamkeit dieser wichtigen Aufsichtsstellen erheblich beeinträchtigen. Die Behörden, die die Grundrechte im Rahmen des KI-Gesetzes schützen, müssen in der Lage sein, unabhängig und effektiv Aufsicht über risikoreiche Systeme führen zu können. Dazu zählen insbesondere solche, die in hochsensiblen Bereichen wie Strafverfolgung, Migration und Grenzkontrolle eingesetzt werden. Ihre Anfragen an die Marktüberwachungsbehörden (MSAs) oder Unternehmen sind eine der wichtigsten Säulen der Aufsicht über diese hochsensiblen Bereiche risikoreicher Systeme.

Zudem erreicht der Vorschlag nicht das Ziel der „Vereinfachung", da es aus einem simplen Verfahren mit einem Schritt (eine Artikel-77-Stelle fragt Informationen vom Anbieter an)

ein komplizierteres Verfahren mit zwei Schritten macht (die Artikel-77-Stelle fragt die MSA, die dann den Anbieter fragt).

Was wir empfehlen:

- Die Änderung von Artikel 77 sollte gestrichen werden.

Änderungen an der Open Data-Richtlinie

14. Nutzung von offenen Standardlizenzen stärken.

Relevante Artikel: Art. 32r, 32q, Erwägungsgründe 25 und 26 Data-Act-E.

Worum es geht: Der Digitale Omnibus zielt darauf ab, die EU-Datenvorschriften zu vereinfachen, indem die Open Data-Richtlinie in das Datengesetz integriert wird. Neben dieser sinnvollen Bündelung wurden allerdings neue substantielle Änderungen eingebracht. Öffentliche Stellen sollen besondere Bedingungen und Kosten an die Weiterverwendung offener Regierungsdaten knüpfen können, etwa für “sehr große Unternehmen”, insbesondere Gatekeeper nach dem DMA.

Warum das wichtig ist: Die Änderungen schwächen den Grundsatz „Open by Default“ und machen den offenen Zugang zu Informationen komplizierter statt einfacher. Aktuell werden offene Regierungsdaten häufig unter Standardlizenzen veröffentlicht. Besonders wichtig und international anerkannt sind die CC0 und CC-BY Lizenzen. Beide erlauben keine Diskriminierung bei der Weiterverwendung. Die Änderungen können öffentliche Stellen dazu veranlassen, offene Lizenzen aufzugeben und neue bedingte Lizenzen einzuführen. Dadurch wäre es schwierig oder unmöglich, diese Quellen mit Daten aus anderen Quellen zu kombinieren oder in offenen Projekten wiederzuverwenden.

Offene Projekte wie die Wikipedia oder OpenStreetMap spielen aber eine entscheidende Rolle in den Bereichen Bildung, Forschung und freiem Zugang zu Wissen und sind auf Inhalte, die unter standardmäßigen offenen Lizenzen (wie CC0 und CC-BY) veröffentlicht werden, angewiesen. Die EU würde damit ohne Not existierende digitale öffentliche Güter (Digital Public Goods) mit einer starken Basis an Freiwilligen in Europa die Arbeit erheblich erschweren oder sogar unmöglich machen, neue Rechtsunsicherheit schaffen und Interoperabilität im Rahmen der offenen Daten erschweren. Dies kann gerade bei internationalen Projekten zu erheblichem Aufwand und Kosten führen.

Der Vorschlag geht fälschlicherweise davon aus, dass öffentliche Stellen auf Lizenzbeschränkungen angewiesen sind, um „sehr großen Unternehmen“ die Bereitstellung und Weiterverwendung von Daten in Rechnung zu stellen. Die Erhebung von Gebühren kann jedoch unabhängig von der Lizenzierung erfolgen und somit die oben beschriebenen Probleme vermeiden. Wir teilen das Ziel, bestehende ökonomische Asymmetrien zu adressieren. Dieses Problem sollte jedoch nicht über Lizenzen gelöst werden. Es gibt alternative Möglichkeiten, etwa unterschiedliche Gebühren für auf unterschiedliche Bedarfe spezialisierte API Zugänge, die etwa Infoboxen, Abschnitte, Tabellen oder Referenzen maschinenlesbar aufbereiten, eine Praxis, die etwa Wikimedia Enterprise für die Bedarfe von großen Sprachmodellen eingeführt hat.

Was wir empfehlen:

- Akteursspezifische Lizenzbedingungen in Art. 32r Abs. 4 sollten gestrichen werden. Sollte weiterhin Handlungsbedarf gesehen werden, sollte auf eine differenzierte Gebührenerhebung gemäß Art. 32q Abs. 6 zurückgegriffen werden. Hierzu könnten Kosten für den Zugang von “sehr großen Unternehmen” über APIs oder Massendownloads erhoben werden. Eine detaillierte Beschreibung dieses Vorschlages findet sich in der Zusammenfassung von Communia, Wikimedia Europe und Creative Commons.
- Artikel 32r Abs. 3 sollte Mitgliedstaaten dazu auffordern, die Verwendung international anerkannter Standardlizenzen zu fördern, im Sinne einer Präzisierung der bisherigen Regelung aus Art. 8 Abs 2 Open Data-Richtlinie.