BÜNDNIS F5

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

info@buendnis-f5.de

Kommentierung Digitales Omnibuspaket 2025 der EU Kommission

Berlin, den 14. Oktober 2025

Executive Summary

Das digitale Omnibuspaket bietet die Chance, das EU-Digitalrecht zu vereinfachen. Damit diese Reform nicht zu einer Schwächung der Grundrechte führt, sollte der Fokus auf der konsequenten Durchsetzung und kohärenten Anwendung des bestehenden Rechtsrahmens liegen. Ein interoperabler Ansatz kann Überschneidungen verringern und gleichzeitig klare Zuständigkeiten und Schutzstandards bewahren. Ziel sollte Kompatibilität statt Umkehrung sein: Bestehende Regeln besser verzahnen, anstatt sie aufzuweichen oder gegeneinander auszuspielen. Die Bundesregierung kann mit dieser Haltung als konstruktive Stimme auftreten, die sich für Vertrauen und Rechtssicherheit stark macht.

1. Einleitung:

Die Europäische Union ist in den letzten Jahren mutig vorangegangen und hat im Bereich der Digitalgesetzgebung unter anderem mit DSA, DMA und AI Act wichtige Grundpfeiler mit globaler Strahlkraft etabliert. Mit der beginnenden Umsetzung auf nationaler Ebene herrschte weitgehend Einigkeit: Nun kommt es auf eine **stabile und konsistente Anwendung des EU-Digitalrechts** an. Nur so entsteht für alle Akteure echte Rechts- und Planungssicherheit. Dies hängt wesentlich von klaren Leitlinien der nationalen Aufsichtsbehörden und einer kohärenten Koordination auf europäischer Ebene ab.

Das digitale Omnibuspaket der Europäischen Kommission bietet die wichtige Möglichkeit, das bestehende EU-Digitalrecht besser aufeinander abzustimmen. Das vorgeschlagene **Digitale Omnibus-Paket als Teil des Simplification Package** droht diese Rechtssicherheit jedoch zu destabilisieren. Wir plädieren daher ausdrücklich für eine konsequente **Durchsetzung und kohärente Anwendung des bestehenden Rechts**, statt für vorschnelle Änderungen des Rechtsrahmens. Dies gilt umso mehr, da in vielen Mitgliedstaaten bislang nicht einmal die zuständigen Aufsichtsbehörden für

Data Act und AI Act benannt wurden. Eine Reform an dieser Stelle würde Unsicherheit eher verstärken als abbauen.

2. Grundsätzliche Bewertung:

Der Digital-Omnibus bietet die Chance, das europäische Digitalrecht zu verbessern – allerdings nur, wenn er Rechtsklarheit schafft, ohne das Schutzniveau zu senken und Verantwortlichkeiten aufzuweichen. Erste Diskussionen deuten jedoch auf eine Verschiebung von juristischen Präzisierungen hin zu materiell-rechtlichen Eingriffen hin und damit auf eine mögliche Aushöhlung von Grundrechten im Namen der Vereinfachung. Dies bewerten wir kritisch und plädieren stattdessen für den Erhalt des bisherigen Schutzniveaus und klaren Verantwortlichkeiten. Denn eine nachhaltige, gemeinwohlorientierte Digitalisierung erfordert kohärente Regulierung, klare Zuständigkeiten und nicht zuletzt die aktive Einbindung der Zivilgesellschaft. Zivilgesellschaftliche Akteure können aus gemeinwohlorientierter Perspektive auf zentrale Widersprüche im bestehenden Rechtsrahmen hinweisen. Diese Perspektive ist entscheidend, um Regulierung praxisnah und grundrechtsbasiert weiterzuentwickeln.

3. Data Acquis (Data Governance Act, Free Flow of Non-Personal Data Regulation, Open Data Directive)

Erhaltung essenzieller Trennlinien bei ODD und DGA: Die ODD verfolgt das wichtige Ziel, nicht-vertrauliche Informationen aus öffentlichen Stellen möglichst umfassend zugänglich und nachnutzbar zu machen („open by default“). Der DGA hingegen regelt sensible Datenbestände wie vertrauliche oder personenbezogene Informationen. Hier darf der Zugang nur ausnahmsweise, bei nachgewiesenem Bedarf und unter strengen Schutzauflagen erfolgen. Der Vorschlag, die Open-Data-Richtlinie (ODD) mit Kapitel II des Data Governance Act (DGA) zusammenzuführen, birgt entsprechend das Risiko, die zentrale Unterscheidung zwischen „standardmäßig offenen“ Datensätzen und „standardmäßig geschützten“ Datensätzen unklar zu machen. Eine Vermischung dieser Logiken könnte zu einer systematischen Schwächung des Datenschutzes und der Datensicherheit führen, die als wichtige Prinzipien jedoch dringend gewahrt werden müssen.

Übertragung des bestehenden DGA-Rahmen auf die DSGVO: Das geltende Regelwerk des DGA bietet eine gute Grundlage, enthält jedoch auch Schwachstellen,

die in der Praxis die Durchsetzung der DSGVO untergraben können. Diese beziehen sich vor allem auf die Punkte Einwilligung, Zweckbindung, Gemischte Datensätze und Weitergabe. Im Kontext der **Einwilligungen** arbeitet der DGA mit unklaren Begrifflichkeiten und ersetzt teils den klar definierten Begriff der „Einwilligung" durch vage Formulierungen wie „Erlaubnis", was in der Konsequenz zu Rechtsunsicherheit führt. Bei der **Zweckbindung** bestimmt die zentrale Datenschutzvorgabe, dass Daten nur für einen klar bestimmten Zweck genutzt werden dürfen. Dies wird allerdings nicht hinreichend abgesichert. Für **gemischte Datensätze,** die sowohl offene als auch vertrauliche Informationen enthalten, fehlen klare rechtliche Leitlinien. Zudem ist bei der **Weitergabe**, also nach der Freigabe durch eine öffentliche Stelle unklar, welche Schutzmechanismen bei den datenverarbeitenden Akteuren greifen sollen. Bei einer möglichen Harmonisierung von DGA und DSGVO ist es daher essentiell, die bestehenden Schwachstellen zu berücksichtigen.

4. Cookies und andere Tracking-Technologien nach der ePrivacy-Richtlinie

Reform im Sinne der Grundrechte: Die Diskussion um Cookies zeigt exemplarisch, wo die Möglichkeiten einer konsequenten Durchsetzung im Sinne der Grundrechte liegen. Seit Einführung der DSGVO arbeiten Consent Management Platforms (CMPs) gezielt daran, die individuelle Durchsetzung informationeller Selbstbestimmung zu umgehen. Cookie-Banner werden technisch so gestaltet, dass Nutzerrechte schwer ausübbar sind: Interfaces verstecken sich in Shadow-DOMs und verschachtelten iframes, Klassen und IDs ändern sich bei jedem Laden, Texte und Schalter werden asynchron nachgeladen. Dazu kommen A/B-Tests, die Abläufe laufend variieren.

Diese Auswahl müsste dann verpflichtend über eine Schnittstelle bereitgestellt werden, die von den Browsern den CMPs zugänglich gemacht wird. Auf diese Weise ließe sich das **Recht auf informationelle Selbstbestimmung** nicht nur rechtlich, sondern auch praktisch wirksam umsetzen. Eine Möglichkeit, neue und bessere Verantwortlichkeiten zu schaffen, bestünde darin, Browser dazu zu verpflichten, eine **Abfrage bei den Nutzer:innen zu grundlegenden Cookie-Kategorien** einzublenden – etwa „technisch notwendig" (auch wenn das immer wieder umstritten ist und in vielen Fällen Klärung bedarf), „kommerzielle Nutzung" oder „Nutzung zur Verbesserung der Anwenderfreundlichkeit".

Rechtlicher Rahmen und notwendige Konsequenzen: Art. 5(3) ePrivacy-Richtlinie ist ein Grundpfeiler des EU-Digitalrechtsschutzes: Er schützt Privatsphäre und Vertraulichkeit der Kommunikation, indem er für jeden Zugriff auf Geräteinhalte eine vorherige Einwilligung verlangt – unabhängig davon, ob personenbezogene oder nicht-personenbezogene Daten betroffen sind. Damit ergänzt er die DSGVO als *lex specialis* und sichert die Unverletzlichkeit von Geräten und Kommunikation gegen kommerzielle wie staatliche Eingriffe.

Eine Aufweichung — etwa durch „berechtigtes Interesse“ oder neue Ausnahmen für Statistik- oder Reichweitenmessung — würde diesen Kernschutz aushöhlen und invasive Praktiken legitimieren. „Consent Fatigue“ entsteht nicht durch zu strenge Regeln, sondern durch irreführende Oberflächen der CMPs.

5. Interoperabler Ansatz bei Cybersicherheitsvorfällen

Interoperabilität: Ein interoperabler Ansatz kann anstelle einer Zusammenlegung von Gesetzgebung sicherstellen, dass Prozesse so abgestimmt werden können, dass Doppelarbeit für Unternehmen vermieden wird, während getrennte Meldekanäle und klare Zuständigkeiten erhalten bleiben. Dies reduziert Bürokratie, ohne die Grundrechtsgarantien der DSGVO zu schwächen.

Die Meldepflichten nach NIS2 und DSGVO verfolgen unterschiedliche, komplementäre Ziele. Die **DSGVO** dient dem Schutz der Grundrechte und Freiheiten, mit klar risikobasierten Pflichten zur Meldung von Datenschutzverletzungen an Aufsichtsbehörden und ggf. betroffene Personen. Auf der anderen Seite zielt **NIS 2** auf die Stärkung der Integrität und Resilienz von IT-Systemen, mit Fokus auf Cybersicherheit. Eine Vereinfachung sollte diese Funktionen ergänzen. Ein einheitliches Meldeportal oder übermäßige Integration könnten dazu führen, dass Datenschutzaspekte hinter technischen Vorfällen zurücktreten. Zudem würde dieses Meldeportal die Gefahr umgehen, dass Datenschutzaufsichtsbehörden mit Meldungen außerhalb ihres Mandats überlastet werden, während sie wichtige Informationen priorisieren können.

6. Umsetzung der KI-Verordnung ermöglichen statt Schutzmaßnahmen gegen risikoreiche KI-Systeme abzubauen

Grundrechtskonforme Vereinfachung: Um einen grundrechtskonformen Weg der Vereinfachung zu gehen, müssen der Zugang zu Rechtsberatung ausgebaut, die Ausnahmeregelungen für RBI-Systeme in Art. 5 (h) AI Act aufgehoben und weitere Orientierungshilfen für die Implementierung bereitgestellt werden, etwa durch delegierte Rechtsakte. Simplifizierung darf also nicht Deregulierung bedeuten.

Evaluierung auf Grundlage von Fakten, nicht Hypothesen: Die KI-Verordnung ist noch nicht vollständig in Kraft getreten, sodass noch keine aussagekräftigen Belege für ihre Auswirkungen oder mögliche Mängel gefunden werden können. Das **Bekenntnis der EU zu Better Regulation** erfordert eine faktenbasierte Bewertung von Gesetzen, während derzeitige materielle Änderungen nur auf Grundlage von Hypothesen geschlossen werden können.

Rechtsunsicherheiten vermeiden und konsistente Anwendung von Vorgaben fördern: Unternehmen haben sich mindestens seit einem Jahr auf die Einhaltung der KI-Verordnung vorbereitet und Prozesse und Sicherheitsvorkehrungen im Einklang damit entwickelt. Die vorgeschlagene „Vereinfachung“ ohne evidenzbasierte Bewertung bestehender Maßnahmen schafft mehr Unsicherheit für Unternehmen und könnte sogar diejenigen „bestrafen“, die die Gesetzgebung frühzeitig umgesetzt haben, Im Zweifel könnte die europäische Industrie am meisten unter einer Deregulierung im Bereich KI zu leiden haben.

Viele der Vorgaben wie beispielsweise die Einführung der Grundrechte-Folgenabschätzung (FRIA) für Betreiber stellen außerdem sicher, dass diese die besonderen kontextbezogenen Risiken in ihrem Land oder Einsatzkontext berücksichtigen. Ohne eine FRIA laufen Betreiber Gefahr, wichtige kontextbezogene Aspekte zu übersehen und unbeabsichtigt zur Verletzung von Grundrechten beizutragen. Durch die Vorgabe solcher Sorgfaltsstandards für Hochrisikobereiche schafft das KI-Gesetz eine Grundlage für die grundlegende Qualitätskontrolle von KI-Systemen auf dem EU-Markt. Eine „Vereinfachung“ dieser Anforderungen würde eine Senkung der Messlatte für Hochrisikobereiche bedeuten und würde in der Tat Anbieter benachteiligen, die sich an die höchsten Standards für eine verantwortungsvolle Entwicklung halten wollen, da weniger sorgfältige Wettbewerber sie unterbieten könnten, was zu weniger vertrauenswürdigen Systemen auf dem EU-Markt führen würde.

AlgorithmWatch
Gesellschaft für Freiheitsrechte
Open Knowledge Foundation
Reporter ohne Grenzen
Wikimedia Deutschland
info@buendnis-f5.de

7. European Digital Identity Framework & EU Business Wallet

Weiterentwicklung von Digitalen Identitäten: Die Weiterentwicklung des europäischen Rahmens für digitale Identitäten bietet die Möglichkeit, Kosten zu senken und Rechtssicherheit zu erhöhen, ohne dabei Schutzstandards zu senken. Damit das geplante **EUID-Wallet** von Bürger:innen angenommen wird, ist **Vertrauen** zentral — Vertrauen, dass die Wallet ihre Identität nicht mit sämtlichen Online-Aktivitäten verknüpft. Dieses Vertrauen muss sich nicht nur auf die Architektur der Wallet selbst erstrecken, sondern auch auf **relying parties** und andere zentrale Akteure wie qualifizierte Vertrauensdiensteanbieter.

Die geplante EU Business Wallet sollte von Beginn an so gestaltet werden, dass sie **kompatibel mit der bestehenden EUID-Wallet** ist. Es besteht kein Bedarf, bestehende Regeln „zu verschlanken", da es für die Business Wallet noch keine Überschneidungen gibt. **Die Prinzipien für anonyme Nutzung** dürfen außerdem nicht geschwächt werden. Auch die **Meldepflichten für relying parties** müssen erhalten bleiben, um Missbrauch zu verhindern. Zudem ist es zentral, **Freiwilligkeit** zu wahren**:** Die Nutzung der EUID-Wallet muss stets freiwillig bleiben. Jede direkte oder indirekte Diskriminierung von Personen, die andere Identifikationsmittel nutzen, wäre problematisch — besonders in Hinblick auf **digital divides** und die Gefahr von Exklusion und Marginalisierung. Ein (tatsächlicher oder wahrgenommener) Zwang zur Nutzung würde das Vertrauen und damit die Verbreitung erheblich beeinträchtigen.

8. Haushaltsverknüpfung und Durchsetzungsfähigkeit

Eine kohärente und glaubwürdige Digitalpolitik setzt eine ausreichende finanzielle Ausstattung der Aufsichts- und Durchsetzungsbehörden voraus. Die konsequente Umsetzung zentraler EU-Digitalgesetze kann nur gelingen, wenn die zuständigen Stellen über die notwendigen personellen und finanziellen Ressourcen verfügen. Kürzungen, etwa im Budget der Bundesnetzagentur, können Glaubwürdigkeit und Wirksamkeit der Regulierung gefährden. Die Bundesregierung sollte sich dafür einsetzen, dass Durchsetzungsstrukturen auf allen Ebenen im Haushalt abgesichert und Synergien zwischen den Behörden gestärkt werden.