English version below (p. 23)

Frankfurt School
Frankfurt Competence Centre for
German and Global Regulation (FCCR)

09.03.2026

Reform der Regulierung für Wettbewerbsfähigkeit und digitale Souveränität

Positionspapier des FCCR zum „Digital Omnibus“

R. Koch/T. Weck (Verf.)*
A. Diefenhardt/M. Jager/J. Redenius-Hövermann

1. Einleitung: Notwendigkeit einer konzeptionellen Neuorientierung

Das am 19. November 2025 vorgestellte „Digital Omnibus“-Paket der Europäischen Kommission markiert einen ***Wendepunkt für die Digitalpolitik*** der Europäischen Union (EU). Zwar ist das erklärte Ziel, die Regulierung zu vereinfachen und damit die Wettbewerbsfähigkeit der europäischen Wirtschaft zu stärken, zu begrüßen. Der gegenwärtige Regulierungsansatz – einschließlich der im Omnibus vorgeschlagenen schrittweisen Änderungen – reicht aber nicht aus, um den Herausforderungen der globalen digitalen Landschaft gerecht zu werden. Die ***Regulierung*** der letzten Jahre hat sich zu einem „Dickicht“ entwickelt, das ***von den Betroffenen nicht mehr durchblickt*** werden kann und damit die Freiräume für selbstbestimmtes Verhalten übermäßig einschränkt. Der Regelungsrahmen der EU bedarf deshalb mehr als nur geringfügiger Anpassungen; er erfordert eine grundlegende konzeptionelle ***Neuausrichtung***.

Die EU sollte über Einzeländerungen hinaus eine neue, datennutzungsfreundliche Regulierungsphilosophie entwickeln, die gleichzeitig die Grundrechte strikt wahrt. Diese Neuorientierung ist notwendig, um das komplexe ***Zusammenspiel zweier zentraler politischer Ziele*** zu bewältigen: das Bestreben der Kommission, die Wettbewerbsfähigkeit von Unternehmen zu stärken, und das Bestreben von EU und Bundesregierung, die digitale Souveränität auszubauen. Dabei ist entscheidend zu erkennen, dass diese beiden Ziele nicht gleichzusetzen sind. Eine nüchterne Kritik des bestehenden Rahmens ist der notwendige erste Schritt zur Entwicklung einer kohärenteren und effektiveren Strategie.

2. Kritik am geltenden EU-Rechtsrahmen für digitale Technologien

Um einen neuen Kurs einzuschlagen, ist es unerlässlich, zunächst die ***systemischen Mängel des bisherigen EU-Ansatzes*** zur digitalen Regulierung zu verstehen. Diese Defizite sind keine isolierten Probleme, sondern miteinander verknüpfte Schwierigkeiten, die erhebliche Rechtsunsicherheit schaffen, Innovationen hemmen und letztlich Wettbewerbsfähigkeit und Souveränität untergraben. Der vorherrschende Rahmen ist durch vier Hauptmängel gekennzeichnet:

- **Zielkonflikte:** Wichtige Regelungen wie die Datenschutz-Grundverordnung (DSGVO) und das KI-Gesetz versuchen, mehrere Ziele gleichzeitig zu verfolgen, ohne dass der Gesetzgeber selbst dazwischen hinreichend abwägt. Sie vermischen die Erfüllung staatlicher Aufgaben (z. B. die Gewährleistung eines funktionierenden Binnenmarktes) mit dem Schutz privater Interessen (z. B. individueller

* Roland Koch, Ministerpräsident a.D., ist Management Practice-Professor, Thomas Weck ist Associate Professor am Frankfurt Competence Centre for German and Global Regulation (FCCR) der Frankfurt School of Finance and Management. Die Autoren erklären, dass das FCCR von Unternehmen finanziert wird, die an behördlichen Verfahren zu den hier behandelten Themen auf EU- und/oder nationaler Ebene beteiligt waren oder sind, obwohl es gegenüber seinen Finanzierungspartnern unabhängig ist.

Datenschutzrechte). Diese Zielvermischung führt zu Unklarheiten sowohl hinsichtlich der Ziele der Regulierungen als auch ihrer praktischen Umsetzung.

- **Nichtbeachtung des zivilrechtlichen Rechtsschutzes:** Der aktuelle Rechtsrahmen fokussiert sich auf die administrative Durchsetzung durch öffentliche Behörden, während der zivilrechtliche Schutz von Einzelpersonen und Unternehmen weitgehend ausgeblendet bleibt. Selbst wenn die Regelungen Rechte für Betroffene schaffen, sind die Mechanismen zur Geltendmachung von Rechtsbehelfen vor Zivilgerichten in den Mitgliedstaaten uneinheitlich, was die gesamte Schutzstruktur schwächt.
- **Unterdrückung von Innovationen:** Das EU-Regulierungsmodell ist grundlegend risikoavers geworden und entzieht Unternehmen präventiv wichtige Risikomanagemententscheidungen. Dies schafft ein Klima der Unsicherheit, das Investitionen in neue digitale Geschäftsmodelle hemmt. Fakt ist jedoch, dass führende europäische Unternehmen *trotz* – und nicht wegen – des bestehenden regulatorischen Umfelds oft Innovationen hervorgebracht haben.
- **Fehlende Zukunftsfähigkeit:** Das Regulierungsmodell ist reaktiv und kann mit der technologischen Entwicklung kaum Schritt halten. Das anfängliche Versagen des KI-Gesetzes, den Aufstieg großer Sprachmodelle vorherzusehen, ist ein Paradebeispiel für dieses Defizit. Allein die Notwendigkeit des Digital Omnibus-Pakets – das zur Überarbeitung mehrerer wichtiger, erst in den letzten fünf Jahren verabschiedeter Gesetze geschaffen wurde – ist ein Eingeständnis, dass der aktuelle Ansatz weder agil noch zukunftsorientiert oder nachhaltig ist.

Diese systemischen Mängel zeigen, dass ein neuer, logischer strukturierter Ansatz für die digitale Regulierung nicht nur wünschenswert, sondern zwingend erforderlich ist.

3. Ein Vorschlag für einen regulatorischen Neuansatz: Differenzierung der Regulierung nach Adressat und Funktion

Als konstruktive Alternative zum aktuellen Modell schlägt das FCCR einen Rahmen vor, der vom monolithischen Ansatz zur Datenregulierung – ausgehend von der DSGVO – abrückt. Ein effektiveres System muss seine ***Regeln anhand der beteiligten Akteure*** (des „Adressaten“) ***und des jeweiligen Kontexts der Dateninteraktion*** (der „Funktion“) differenzieren. Dies ermöglicht eine zielgerichtete, verhältnismäßige und logisch konsistente Regulierung in verschiedenen Bereichen der digitalen Wirtschaft.

a) Hoheitliche Grundrechtseingriffe

Wenn der Staat in seiner Hoheitsgewalt auf personenbezogene Daten zugreift, steht der ***Schutz der Grundrechte*** vor staatlichen Eingriffen auch weiterhin im Vordergrund. In diesem Kontext bieten die DSGVO und die nationalen Datenschutzgesetze einen geeigneten und bewährten Regelungsrahmen. Sie schaffen ein ausgewogenes Verhältnis zwischen der Ermöglichung legitimer staatlicher Aufgaben und dem Schutz der Rechte des Einzelnen. Für diese staatlichen Maßnahmen sollten die bestehenden Regelungen unberührt bleiben. Dennoch ließen sich Effizienzpotentiale heben, wenn andere Stellen der öffentlichen Verwaltung ***schon vorhandene Daten*** für die Erfüllung ihrer gesetzlichen Aufgaben nutzen dürften. Dies sollte jedenfalls gelten, wenn sich dadurch Doppelerhebungen vermeiden lassen und keine grundlegenden Schutzinteressen verletzt werden.

b) Nutzung von Unternehmensdaten im Umgang mit Verbrauchern

Im Geschäftsverkehr zwischen Unternehmen und Verbrauchern stellt sich die regulatorische Herausforderung anders dar. Hier stehen die Verbraucher nicht unter staatlicher Kontrolle, sondern üben ihre Vertragsfreiheit aus. Kernproblem ist das ***strukturelle Ungleichgewicht der Verhandlungsmacht*** zwischen den beiden Parteien. Die derzeitige Einwilligungspraxis nach der DSGVO (Art. 6 Abs. 1 Buchst. a) ist in diesem Kontext ineffektiv; sie trägt dem erheblichen ***Informationsdefizit der Verbraucher*** nicht Rechnung und führt letztlich dazu, dass die rechtliche Verantwortung durch Mechanismen wie Cookie-Banner auf sie abgewälzt wird. Eine zentrale Steuerung von Einwilligungen z. B. über einen Webbrowser ist schwer zu implementieren, weil Einwilligungen zweckgebunden erteilt werden.

Ein effektiverer Ansatz wäre, ganz vom Einwilligungsmodell abzurücken und den Verbraucherschutz stattdessen auf ein solides Vertrags- und Verbraucherrecht, wie beispielsweise ***standardisierte Geschäftsbedingungen*** (AGB-Recht; vgl. aktuell schon die P2B-Verordnung), zu gründen. Darüber hinaus sollte die ***Aufsicht*** über grenzüberschreitende Online-Dienste national ***in einer einzigen Behörde*** (wie der deutschen Bundesnetzagentur) gebündelt werden, um eine einheitliche Durchsetzung zu gewährleisten. Ergänzend dazu sollte die Entwicklung der Musterfeststellungsklagen beobachtet werden, um ggf. die ***zivilrechtlichen Rechtsbehelfe*** für Verbraucher nachzujustieren.

c) Datenaustausch zwischen Unternehmen (B2B)

Die ***bestehende Regulierung*** des B2B-Datenaustauschs ist ***weiterhin unzureichend***. Sie geht nicht konsequent genug auf die zentralen Herausforderungen des Marktes ein, nämlich die Gewährleistung technischer Interoperabilität, die Überwindung von Informationsasymmetrien und die Balance zwischen Datenzugriff und dem legitimen Schutz von Geschäftsgeheimnissen. Ein ***praktikableres Modell*** als der Data Act bietet hierfür der ***European Health Data Space*** (EHDS), der ein besseres Gleichgewicht zwischen Datenzugang und Schutz geistigen Eigentums schafft.[1]

d) Datennutzung in Forschung und Entwicklung

Die Fähigkeit, Daten für Forschung und Entwicklung zu nutzen und auszutauschen, ist ein Eckpfeiler der Wettbewerbsfähigkeit. Die aktuelle europäische Landschaft ist jedoch zu fragmentiert und restriktiv. Dies führt dazu, dass Daten gänzlich ungenutzt bleiben oder dass unnötige Mehrfacherhebungen (entgegen dem *Once-only*-Prinzip) stattfinden. Um Innovationspotenziale freizusetzen, ist ein effizienterer Ansatz erforderlich. Zu den wichtigsten Reformen sollten gehören:

- **Konsolidierung und Vereinfachung** der Vielzahl von Datenzugriffsregeln, die für öffentliche Stellen im Rahmen von Richtlinien wie der Public Sector Information (PSI) Directive, INSPIRE und anderen gelten.
- **In Deutschland** wird staatlichen Stellen die Datennutzung in ihrem Aufgabenbereich unter Beachtung der Datenschutzgesetze gestattet. Der Anwendungsbereich des kommenden Forschungsdatengesetzes wird erweitert, um den Zugang auch zu Daten aller Ressortforschungseinrichtungen zu ermöglichen.

[1] Die straffe Regelung in § 393 SGB V kann ergänzend für Fragen der Cloud-Nutzung herangezogen werden.

- **Auf EU-Ebene** werden konzertierte Anstrengungen unternommen, um die Fragmentierung der Datenzugangsnormen zu verringern und einen kohärenteren Rahmen für Forscher zu schaffen.

Des Weiteren sind die Instrumente des ***Data Governance Act (DGA)*** für Forschung und Entwicklung ***nur bedingt geeignet.*** Die Annahme, Vertrauen in Datennutzung entstehe primär durch die Regulierung von Intermediären, greift zu kurz. Entscheidend ist vielmehr die Vertrauenswürdigkeit der Datenquelle und die rechtssichere Begrenzung der Datennutzung. Hier erscheint die im Digital Omnibus vorgeschlagene ***„European Business Wallet" vielversprechender***. Voraussetzung wäre jedoch, dass Forschungsinstitutionen eine einheitliche Kennung erwerben können und ein frei einsehbares Verzeichnis eingerichtet wird, das über Nutzungsbeschränkungen für EBW-Signaturen Auskunft gibt.

e) Regulierung künstlicher Intelligenz

Das KI-Gesetz ist in seiner jetzigen Form grundlegend fehlerhaft. Es schafft eine ***zusätzliche Regulierungsebene*** zusätzlich zu den bestehenden Produktsicherheits- und Haftungsgesetzen und etabliert ein belastendes, überwachungsähnliches Compliance-System, das ***für einen schnelllebigen Technologiesektor ungeeignet*** ist.

Das Kernproblem des Gesetzes liegt darin, dass es sich auf die ***Risiken von KI-Outputs*** und deren Generierung konzentriert, ***ohne*** jedoch ***Rechtssicherheit für die Inputs*** zu schaffen, die für die KI-Entwicklung und Innovationen entscheidend sind – insbesondere die Verwendung personenbezogener Daten, urheberrechtlich geschützter Inhalte und Geschäftsgeheimnisse für das Training von Modellen. Dies versetzt Innovatoren in eine rechtliche Grauzone. Das KI-Gesetz sendet somit ein äußerst ***negatives Signal an den Markt*** und behindert direkt die Ziele der EU, Wettbewerbsfähigkeit und digitale Souveränität zu stärken. Das Gesetz muss grundlegend überarbeitet werden, um ein tragfähiges Gleichgewicht zwischen Risikomanagement und Innovation herzustellen, oder gar vollständig aufgehoben werden.

4. Die Rückgewinnung der digitalen Souveränität als staatliches Gebot

Für eine wirksame Politikgestaltung ist es unerlässlich, zunächst den Begriff der „digitalen Souveränität" korrekt zu definieren. Es handelt sich dabei um ein ***staatliches Interesse,*** das darauf abzielt, die Abhängigkeit von ausländisch kontrollierter kritischer digitaler Infrastruktur zu verringern. Dies unterscheidet sich grundlegend vom ***Unternehmensinteresse an Wettbewerbsfähigkeit***. Die aktuelle Position der Bundesregierung, die diese beiden Konzepte vermischt, beruht auf einem Missverständnis und schwächt ihre strategische Ausrichtung.

Unter dem Gesichtspunkt digitaler Souveränität sind komplexe Regulierungen wie der ***Digital Markets Act*** (DMA) ***und der Digital Services Act*** (DSA) kein Zeichen europäischer Wehrhaftigkeit als vielmehr ein ***Symptom langjährigen politischen Versagens****:* Die Politik hat das Kernproblem unzureichender Rechtsdurchsetzung im Wettbewerbs- und Plattformbereich über Jahre nicht erkannt oder adressiert – Verfahren gegen große US-Plattformen dauerten teils ein Jahrzehnt. Zusätzliche Verhaltenspflichten wie nun in DMA und DSA, die ihrerseits durchgesetzt werden müssen, beheben das eigentliche ***Vollzugsdefizit*** nicht. Zugleich erschöpfen sich diese Regelwerke weitgehend in ***Symbolpolitik***, weil sie an zentralen strukturellen Herausforderungen – insbesondere der auf personenbezogenen Daten beruhenden Geschäftsmodelle und der mangelnden Wirksamkeit der

DSGVO-Einwilligung – nichts ändern; der DMA übernimmt vielmehr sogar die defizitäre Einwilligungslogik und bleibt damit hinter einem wirksamen Verbraucherschutz.

Eine ***echte Strategie*** für digitale Souveränität muss proaktiv und strukturell sein. Sie erfordert die Konzentration auf vier Schlüsselmaßnahmen:

1. **Dezentralisierung der digitalen Infrastruktur** , insbesondere für zentrale staatliche Funktionen (Verwaltung, Sicherheit) und in kritischen Wirtschaftssektoren wie Energie und Finanzen.
2. **Förderung offener Protokolle und Standards,** um die technische Interoperabilität zu erhöhen, die Abhängigkeit von einzelnen Anbietern zu verringern und ein wettbewerbsfähigeres und widerstandsfähigeres Ökosystem zu schaffen.
3. **Die Stärkung effektiver Rechtsdurchsetzung,** indem sichergestellt wird, dass die Regeln einfach und klar sind, die Sanktionen so gestaltet sind, dass sie Verstöße neutralisieren, und die Justizsysteme über ausreichende Ressourcen verfügen, um komplexe digitale Fälle zügig zu bearbeiten.[2]
4. **Die politische Dynamik** für diese Veränderungen sollte durch transparente Offenlegung der laufenden finanziellen und strategischen Kosten verstärkt werden, die sich aus den Abhängigkeiten von ausländischen digitalen Diensten und Infrastrukturen (z. B. aufgrund von Lizenzbindungen) ergeben.

Diese strategische Vision auf hoher Ebene liefert den notwendigen Kontext für die Bewertung der konkreten Vorschläge im „Digital Omnibus“-Paket.

5. Analyse und Empfehlungen für das digitale Omnibuspaket

Dieser Abschnitt bietet eine gezielte Kritik der ***konkreten Gesetzesvorschläge*** zu Daten und KI im Rahmen des Digital Omnibus-Pakets. Während einige der vorgeschlagenen Änderungen vorteilhaft sind, verfestigen viele entweder die oben skizzierte fehlerhafte Regulierungsphilosophie oder führen zu neuen Problemen, die die Rechtslage weiter verkomplizieren werden.

a) Vorgeschlagene Änderungen des Datengesetzes (Data Act)

Die Änderungen des Datengesetzes sind ein ***gemischtes Bild:*** Sie verbinden sinnvolle Konsolidierung mit dem Erhalt gescheiterter Konzepte.

- **Positiv:** Die Zusammenführung verschiedener verwandter Rechtsakte (wie der Verordnung über den freien Datenverkehr nicht-personenbezogener Daten, des Daten-Governance-Rechtsakts und des Datengesetzes) in einem einzigen Instrument ist ein sinnvoller Schritt zur Vereinfachung. Ebenso ist die Einführung von Maßnahmen zum Schutz öffentlicher Daten vor unkontrolliertem Zugriff durch Drittländer ein begrüßenswerter Schritt zur Stärkung der Resilienz.
- **Negativ:** Die Entscheidung, die gescheiterten DGA-Regeln zu Datenintermediären und Datenaltruismus zu übernehmen, ist ein schwerwiegender Fehler. Diese Bestimmungen haben sich als ineffektiv und marktfremd erwiesen und sollten gestrichen, nicht integriert werden. Darüber hinaus sind die neuen Regeln zum Schutz von Geschäftsgeheimnissen unpraktisch, und die Schaffung mehrerer,

[2] Das aktuelle Kommissionsverfahren zur ggf. missbräuchlichen Nutzung geschützter Online-Inhalte für KI (Art. 102 AEUV; nicht: DMA) könnte genutzt werden, um das Wettbewerbsrecht als international akzeptiertes Rechtsinstrument effektiv im Kontext neuer Technologien einzusetzen.

sich überschneidender Definitionen für kleine und mittlere Unternehmen führt zu übermäßiger Komplexität.

b) Vorgeschlagene Änderungen der DSGVO und der ePrivacy-Richtlinie

Die vorgeschlagenen Änderungen der DSGVO bergen das Risiko, ***mehr Unsicherheit*** zu schaffen als zu beseitigen.

- Der Vorschlag, eine neue ***„subjektive" Definition*** von personenbezogenen Daten einzuführen, die darauf basiert, ob eine bestimmte Stelle eine Person identifizieren kann, etabliert einen situationsabhängigen und damit für den Grundrechtsschutz untauglichen Maßstab. Sie würde Rechtsunsicherheit und immense Beweisschwierigkeiten in Rechtsstreitigkeiten schaffen.
- Die Idee eines ***„Drei-Schichten-Modells"***, das unterschiedliche Regeln je nach Unternehmensgröße anwendet, ist abzulehnen. Das Risiko ergibt sich aus der Art der Verarbeitungstätigkeit, nicht aus der Größe des durchführenden Unternehmens. Der Grundsatz muss lauten: „Gleiches Risiko, gleiche Regulierung".
- Die neuen Bestimmungen zur Klärung der Verwendung personenbezogener Daten im ***KI-Training*** sind unzureichend**.** Sie bieten Innovatoren nicht die notwendige Rechtssicherheit und schwächen potenziell den Schutz grundlegender Rechte, ohne die Position der Betroffenen entsprechend zu stärken.

c) Regulierung digitaler Identitäten („European Omnibus Wallet")

Die Einführung einer digitalen Unternehmensidentität ist zu begrüßen. Der im „Digital Omnibus"-Paket vorgelegte Verordnungsvorschlag ist auf das Nötige beschränkt und geht mit wenigen bürokratischen Lasten einher. Allerdings wäre es wünschenswert, dass unionsweit als „einheitliche Kennung" ***auch durch internationale Organisationen entwickelte Kennungen*** anerkannt werden können. Außerdem sollte dafür gesorgt werden, dass nach dem EU-Recht auch ***Forschungsinstitutionen*** eine einheitliche Kennung erwerben können und dass ein ***frei einsehbares Verzeichnis*** eingerichtet wird, das ***über Nutzungsbeschränkungen für EBW-Signaturen*** Auskunft gibt.

Auf ***nationaler Ebene*** gibt es Initiativen – z. B. den Aufbau eines Basisregisters für Unternehmensdaten beim Statistischen Bundesamt[3] – die im Interesse einer umfassenderen und stimmigen Regulierung digitaler Identitäten bei der Ausgestaltung der neuen EU-Gesetzgebung ebenfalls berücksichtigt werden sollten.

d) Vorgeschlagene Änderungen des KI-Gesetzes

Der „Digital Omnibus on AI" bietet lediglich ***oberflächliche Lösungsansätze***, die die grundlegenden Konstruktionsmängel des KI-Gesetzes nicht beheben.

Die Tatsache, dass die Kommission die Notwendigkeit von ***13 zusätzlichen Leitlinien*** zur Präzisierung des Gesetzes angekündigt hat, ist ein stillschweigendes ***Eingeständnis eines gescheiterten Regulierungsansatzes.*** Diese Leitlinien werden den Aufwand für die Einhaltung der Vorschriften für Unternehmen lediglich erhöhen.

Die Schaffung von ***Sonderprivilegien*** für verschiedene Kategorien kleiner Unternehmen ist ein ***weiteres Indiz*** dafür, dass die ***Regulierung für alle zu belastend*** ist. Anstatt

[3] Dazu Unternehmensbasisdatenregistergesetz vom 9. Juli 2021, BGBl. I S. 2506.

komplexe Ausnahmen zu schaffen, sollten die Basisregeln verhältnismäßig und praktikabel sein.

Die Vorschläge beheben nicht die ***vielen Kernprobleme des KI-Gesetzes:*** doppelte Haftungsregelungen, erhebliche Rechtsunsicherheit in Bezug auf Ausbildungsdaten und die abschreckende Wirkung auf Innovationen. Die ***Verzögerung der Anwendung*** des Gesetzes ist zwar ein ***begrüßenswerter taktischer Schritt***, ersetzt aber nicht die notwendige strategische Überarbeitung.

6. Fazit: Wichtigste Empfehlungen für einen überarbeiteten Regulierungsrahmen

Die Europäische Union steht an einem ***Scheideweg.*** Um ihre digitale Zukunft zu sichern, muss sie ihre derzeitige komplexe, risikoscheue und belastende Regulierungspolitik hin zu einem klaren, prinzipienbasierten Rahmenwerk verändern, das Innovationen ermöglicht, den Wettbewerb fördert und die Bürgerinnen und Bürger wirksam schützt. Das „Digital Omnibus"-Paket bietet die Chance, diesen Wandel einzuleiten, jedoch nur, wenn er mit einem tiefgreifenderen Paradigmenwechsel einhergeht.

Die folgenden ***übergeordneten Empfehlungen*** fassen die entscheidenden Maßnahmen zusammen, die für eine erfolgreiche regulatorische Neuausrichtung erforderlich sind:

- **Die DSGVO sollte wieder auf ihren Kernzweck ausgerichtet werden**: den Schutz der Grundrechte im Umgang zwischen Staat und Bürgern. Im Geschäftsverkehr sollten spezifische, zielgerichtete Verbraucher- und Vertragsgesetze genutzt werden, um Machtungleichgewichte zu beseitigen.
- **Förderung des B2B-Datenaustauschs** durch Abschaffung der gescheiterten DGA-Modelle für die Datenvermittlung und stattdessen Fokussierung auf praxisorientierte, branchengeführte Standards für Interoperabilität und den effektiven Schutz von Geschäftsgeheimnissen.
- **Die Datennutzung in Forschung und Entwicklung sollte deutlich vereinfacht und harmonisiert werden.** In Deutschland sollte staatlichen Akteuren die Nutzung vorhandener Daten im Rahmen ihres gesetzlichen Auftrags weiterreichend ermöglicht und der Geltungsbereich des geplanten Forschungsdatengesetzes auf sämtliche Ressortforschungseinrichtungen ausgeweitet werden. Auf EU-Ebene sind koordinierte Initiativen nötig, um die bestehende Fragmentierung abzubauen und Forschenden einen kohärenten, verlässlichen Datenzugang zu eröffnen.
- **Das KI-Gesetz sollte grundlegend überarbeitet werden,** um regulatorische Doppelungen mit bestehenden Haftungsgesetzen zu beseitigen, klare Rechtssicherheit für die Verwendung von Trainingsdaten zu schaffen und die Compliance-Belastungen an nachweisbaren systemischen Risiken auszurichten, nicht an willkürlichen Parametern wie der Unternehmensgröße.
- **Digitale Souveränität als Staatsstrategie verfolgen,** indem man sich auf konkrete, strukturelle Maßnahmen konzentriert – wie die Förderung dezentraler Infrastruktur, offener Standards und die zügige Durchsetzung bestehender Gesetze – anstatt neue Ebenen komplexer und oft symbolischer Regulierung zu schaffen.

* * *

Anhang zum Positionspapier: Stellungnahme zu den Einzelregelungen im Digital-Omnibus-Paket

Die Europäische Kommission hat am 19. November 2025 ihr siebtes Omnibus-Paket vorgestellt und holt dazu Stellungnahmen bis zum 13. März 2026 ein. Dieses Positionspapier nimmt zu den enthaltenen Verordnungsvorschlägen für einen „Digital Omnibus“ zu Daten, einen „Digital Omnibus on AI“ Stellung und einen Verordnungsvorschlag über European Business Wallets Stellung.[4] Die Verordnungsvorschläge liegen bisher nur auf Englisch vor.

a) Digital Omnibus (Daten): Änderungen des Data Act

Vorschrift	Inhalt	Stellungnahme
---	Zusammenfassung von FFDR, DGA, Data Act, Offene-Daten-RL im Data Act	**Zusammenfassung grundsätzlich sinnvoll**, da Systematik zurzeit unklar und Überschneidungen zwischen Rechtsakten. Umwandlung der Offene-Daten-RL in **Verordnungsrecht** aber nicht unproblematisch: Die Kontrolle über Informationen des öffentlichen Sektors, um deren Verfügbarkeit und Weiterverwendung es nach der Richtlinie geht (Erw.-Grd. 16), kann für **innere und äußere Sicherheit der Mitgliedstaaten relevant** sein. **Alternativ** zur Zusammenfassung der Regelungen zur Datenweiterverwendung im Data Act könnten die **DGA-Regelungen** hierzu auch **in die Offene-Daten-Richtlinie integriert** und den Mitgliedstaaten Umsetzungsspielräume belassen werden.
---	Vorratsdatenspeicherung wird getrennt geregelt	Sinnvoll, da **eigenständige Problematik:** Zugriff auf personenbezogene Daten zu Sicherheitszwecken.
Art. 1 Abs. 2(d)	Übernahme der DGA-Regelungen zu Datenvermittlungsdiensten/Datenaltruismus in Data Act	Die Regelungen haben sich **nicht bewährt** und sollten besser ersatzlos wegfallen. Eine spätere Evaluation (Art. 1 Abs. 26 = Art. 49 Data Act n.F.) bietet keinen erkennbaren Mehrwert.

[4] COM(2025) 836 final bzw. COM(2025) 837 final.

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 2(e)	Definition 'medium-sized enterprise'/'small mid-cap'	**Mehrere Kategorien von Kleinunternehmen**, für die Sonderregelungen gelten, **vermindern** die **Rechtsklarheit**. Sie indizieren auch, dass die Regeln des Digital-Omnibus die Wirtschaft weiter übermäßig belasten.
Art. 1 Abs. 3, 4	Einführung eines Weigerungsrechts von Geschäftsgeheimnisinhabern beim Datenzugang (Art. 4 Abs. 8, Art. 5 Abs. 11 Data Act)	Die Verpflichtung von Datenempfängern, die **Geschäftsgeheimnisse** des urspr. Dateninhabers zu schützen, führt zu **schwer zu überblickenden Risiken** für den Dateninhaber. Die Vereinbarung zwischen Produktnutzer und Empfänger stellt insoweit einen Vertrag zulasten Dritter (urspr. Dateninhaber) dar. **Rechtsunsicherheit** durch Kombination **stark wertungsbedürftiger Rechtsbegriffe** („exceptional circumstances", „highly likely" „serious economic damage", „on a case-by-case basis"). Der **Datenzugang** sollte nach Data Act **wie nach EHDS-VO** ausgestaltet werden. Der Regulierungsansatz des Data Act ist insgesamt verfehlt.
Art.1 Abs. 6-14	Begrenzung des Datenzugangs für öffentliche Stellen auf Fälle „öffentlicher Notlagen" anstelle von „außergewöhnlicher Notwendigkeit"	Die Begrenzung **reduziert den** potenziellen **Aufwand** für Unternehmen und erscheint mit Blick auf das Ziel der Wettbewerbsfähigkeit **unproblematisch**.
Art. 1 Abs. 15	Regelungen zu Cloud-Wechsel (Art. 23 ff. Data Act) werden vereinfacht (neuer Art. 31 Abs. 1a, 1b Data Act).	**Regulierungsansatz zu hinterfragen:** Neben Speichern werden sehr spezifische Dienste nachgefragt → Bedarf für isolierte Regeln zum Wechsel in Art. 23 ff. Data Act ist insgesamt unklar. Wechsel wird weniger durch inkompatiblen Funktionsumfang, eher durch inkompatible Softwarearchitekturen/Schnittstellen und Datenformate erschwert.
At. 1 Abs. 16	Wiederverwendung öffentlicher Daten unter Vorbehalt, dass Zugriff von Drittstaaten verhindert werden kann (Art. 32 Data Act)	Sinnvoll zur **Stärkung von Resilienz im EU-Außenverhältnis.** **Ausgestaltung der Regelung aber unklar:** Verweisungen auf sonstige Regelungen, wertungsbedürftige Rechtsbegriffe („minimum amount of data permissible"; „reasonable interpretation")

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 17	Streichung der Regelung über intelligente Verträge (Art. 36 Data Act)	Sinnvoll, die Regelung ist unpraktikabel und führt zu Rechtsunsicherheit (so die EU-Kommission selber; COM(2025) 837 final, S. 5 und Erw.-Grd. 16).
Art. 1 Abs. 18	Übernahme von DGA-Regelungen zu Datenvermittlungsdiensten und Daten-Altruismus	Die **Regelungen** haben sich **nicht bewährt** und sollten anstelle der vorgesehenen Straffung innerhalb des Data Act (Art. 32a ff. n.F.) besser ersatzlos wegfallen. Eine spätere Evaluation (Art. 1 Abs. 26 = Art. 49 Data Act n.F.) bietet keinen erkennbaren Mehrwert.
Art. 1 Abs. 18	Übernahme von DGA-Regelungen zur Wiederverwendung öffentlicher Daten	Die **Übernahme dieser Regelungen (Art. 32i ff. Data Act n.F.) ist sinnvoll**. Dadurch werden für öffentliche Daten einheitliche Standards geschaffen. Die **Zusammenführung mit den Regelungen der Offene Daten-Richtlinie (Art. 32n ff. Data Act n.F.)** ist zwar ebenfalls sinnvoll, wegen der Bedeutung der betroffenen Daten für die souveräne Informationsverwaltung der Mitgliedstaaten aber nicht unproblematisch (s.o. Zeile 1). Insbesondere die Regelungen über die **Identifizierung „hochwertiger Datensätze“** (Art. 14 RL (EU) 2019/1024; Art. 32v Data Act n.F.) enthalten zudem viele wertungsbedürftige Rechtsbegriffe. Sie tragen dadurch **kaum** zur **Rechtssicherheit** bei. Besser wäre ohnehin eine umfassende Vereinheitlichung der Regeln für öffentliche Daten, soweit diese statistisch oder wissenschaftlich nutzbar sind: • Der Datenzugang ist bislang zersplittert geregelt (s.a. RL 2007/2/EG; RL 2003/4/EG); • Doppelungen in Sonderregimes wie z. B. für Gesundheitsdaten (VO 2025/327 – EHDS) sollten für mehr Rechtsklarheit reduziert werden (z. B. zu Rechten/Dokumentation/Complianceanforderungen).
Art. 1 Abs. 18	Übernahme des Datenlokalisierungsverbots der FFDR in den Data Act	Die Übernahme des **Datenlokalisierungsverbots (Art. 32h Data Act n.F.) ist vertretbar**, aber die praktische Bedeutung wohl begrenzt. Der Wegfall der FFDR-Vorschriften zu Verhaltenskodizes über Datenteilung ist wegen der begrenzten Regelungswirkung vertretbar.

Vorschrift	Inhalt	Stellungnahme
		Im Interesse an einer allgemeinen **Förderung von Interoperabilität und einheitlichen Datenformaten** sollte dann jedoch der **Anwendungsbereich der Art. 33 ff. Data Act über Europäische Datenräume hinaus erweitert** werden.

b) Digital Omnibus (Daten): Änderungen von Datenschutz-Grundverordnung (DSGVO)

Im Vorgriff auf die Vorstellung des Digital Omnibus hatte Deutschland der Europäischen Kommission Vorschläge für eine Vereinfachung der DSGVO übermittelt. Dieses **„German proposal for simplification of the GDPR“** wurde von Netzpolitik.org vom 23. Oktober 2025 veröffentlicht und ist nach der Folgenabschätzung zum Digital-Omnibus-Paket in dieses eingeflossen. Deshalb wird es in der folgenden Stellungnahme ebenfalls berücksichtigt.

DSGVO

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
---	Zusammenfassung von DSGVO und e-Privacy-RL 2002/58/EG.	---	Grds. sinnvoll.
---	---	Forderung des besseren Ausgleichs zwischen betroffenen Schutzgütern: • Allg. Persönlichkeitsrecht der Betroffenen einer Datenverarbeitung • Wirtsch. Freiheit/Wissenschafts-Freiheit der Datenverarbeiter	Zusätzlich beachten: • Öffentliches Interesse an Datennutzung bei Erfüllung behördlicher Aufgaben • Digitale Souveränität (Resilienz) gegenüber Nicht-EU-Staaten; aber auch Grenzen f. EU-Industriepolitik (Art. 173 AEUV)

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
Art. 3 Abs. 1	Neufassung der Definition von „personenbezogenen Daten“ (Art. 4 DSGVO):	---	Einführung eines „subjektiven Ansatzes“, der den Geltungsbereich des Gesetzes auf Situationen beschränkt, in denen eine Person von einem bestimmten Unternehmen identifiziert werden kann. Die Neuregelung setzt EuGH C-413/23 P – *EDSB* um. Sie geht aber mit dem Risiko einher, dass **Unternehmen strategisch** zwar für sich selbst ausschließen, dass sie personenbezogene **Daten sammeln**, aber dass sie zugleich sicherstellen, dass Sie ihren Geschäftspartnern Daten zur Verfügung stellen, die dort personenbezogen sein können (ohne dass die Betroffenen mit diesen anderen Unternehmen eine direkte Beziehung haben). Außerdem wird die Beurteilung der Datensammlung nach DSGVO durch stark wertungsbedürftige Begriffe erschwert („not [...] personal [...] where that entity cannot identify the natural person [...] taking into account the means reasonably likely to be used by that entity.“). Insoweit dürfte die Neuregelung **erhebliche Beweisschwierigkeiten** in Streitfällen mit sich bringen. **Besser** wäre es, den **Anwendungsbereich der DSGVO insgesamt genauer an den relevanten Grundrechtsfragen auszurichten** und insbesondere zwischen staatlicher und unternehmerischer Datenverarbeitung zu differenzieren.
---	---	Prüfung eines **3-Layer-Model** (s. z. B. Wendehorst): Umfangreiche Pflichten für Großunternehmen, reguläre Pflichten, verminderte Pflichten/Ausnahmen für KMU	**Abzulehnen: Die Schutzbedürftigkeit Betroffener hängt nicht von der Größe des verarbeitenden Unternehmens, sondern von den Risiken der Verarbeitung ab** („same risk – same regulation“). Datenschutzvorgaben müssen sich zudem auf das Erforderliche beschränken, um mit der unternehmerischen Freiheit (Art. 16 GRCh) vereinbar zu sein. Die erforderlichen Vorgaben können von großen Unternehmen sogar i.d.R. besser umgesetzt werden als von kleineren. Großunternehmen haben hierfür mehr Ressourcen.

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
		und nicht-wirtschaftliche Tätigkeiten prüfen	**Besser** wäre es, den **Anwendungsbereich der DSGVO insgesamt genauer an den relevanten Grundrechtsfragen auszurichten** und insbesondere zwischen staatlicher und unternehmerischer Datenverarbeitung zu differenzieren.
Art. 3 Abs. 2	Rückkopplung des Zweckbindungsgrundsatzes (Art. 5 Abs. 1 lit. b DSGVO) an die Zweckbegrenzungsregelung in Art. 6 Abs. 4 DSGVO	---	Sinnvolle Klarstellung.
Erw.-Grd. 30 f.	Datennutzung für KI-Training sollte als „berechtigtes Interesse“ anerkannt werden.	Safe Harbor, um KI-Systeme DSGVO-konform aufzusetzen.	**Der Digital Omnibus verzichtet auf eine Änderung des Gesetzestextes (Art. 6 Abs. 1 lit. f DSGVO). Die Regelung reicht damit nicht aus zur Schaffung von Rechtssicherheit.** Hierfür wären im Übrigen auch Regelungen für die Nutzung von urheberrechtlich geschützten Inhalten und Geschäftsgeheimnissen für das Training von KI-Modellen erforderlich.
Art. 3 Abs. 3	Einschränkung des Schutzes für bes. geschützte Daten (Art. 9 DSGVO) für Fälle des Trainings von KI-Modellen und für Verarbeitung biometrischer Daten zur Identitätsprüfung	Zugriff auf bes. geschützte Daten (Art. 9 DSGVO) sollte (nur) in Notsituationen (z. B. Pandemie) vereinfacht werden.	Die **Freistellung** der Nutzung besonders geschützter Daten **für Zwecke des KI-Trainings** dient dem Schutz unternehmerischer Freiheit (Art. 16 GRCh) bei der Entwicklung innovativer KI-Produkte, aber **schränkt den Grundrechtsschutz für Betroffene empfindlich ein.** Die **Vorgabe**, dass geeignete („appropriate“) **technische und organisatorische Maßnahmen** getroffen werden müssen, um die Sammlung relevanter Daten zu minimieren und solche Daten zu schützen (Art. 9 Abs. 5 DSGVO n.F.), **reicht nicht aus.** Zusätzlich müsste die Rechtsposition der Betroffenen gestärkt werden, z. B. durch eine Vermutungsregelung in Bezug auf Schäden. Die Vereinbarkeit mit Art. 7, 8 GRCh ist daher zweifelhaft.

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
			Der Unionsgesetzgeber wird mit der Regelung davon abgesehen seiner **Schutzpflicht mit Blick auf Ausbeutungsrisiken** zum Nachteil von Verbrauchern nicht gerecht. Die **Nutzung biometrischer Daten** soll auf Fälle beschränkt sein, in denen die Daten unter **alleiniger Kontrolle des Grundrechtsbetroffenen** stehen. Die Regelung erscheint vertretbar. Der **deutsche Vorschlag ist sinnvoll.**
Art. 3 Abs. 4	Einschränkung der kostenfreien Information über die Datenerhebung bei der betroffenen Person oder anderweitig (Art. 12 Abs. 5 DSGVO).	Beschränkung missbräuchlicher Auskunftsanfragen (Art. 15, 57 DSGVO).	Die Regelung des **Digital Omnibus** schränkt das Recht auf kostenfreie Information für missbräuchliche Auskunftsanfragen ein, wobei die Beweislast für einen Missbrauch beim Datenverarbeiter liegt. Die **Regelung erscheint vertretbar.** Die deutschen Vorschläge sind dagegen zu schwerfällig.
Art. 3 Abs. 5	Begrenzung der Information über die Datenerhebung bei der betroffenen Person (Art. 13 Abs. 4 DSGVO) im Rahmen bestehender Rechtsverhältnisse und bei schon vorhandener Information beim Betroffenen.	Verminderung von Informationspflichten (Art. 13 DSGVO): Unternehmen sollten relevante Informationen nur auf eigener Website vorhalten.	Die **Regelung des Digital Omnibus** schränkt das Recht auf Information in Fällen ein, in denen der Betroffene die Informationen zur Wahrnehmung seiner Rechte nicht benötigt. Die Regelung enthält viele wertungsbedürftige Rechtsbegriffe („clear and circumscribed relationship"; "activity that is not data-intensive"; "reasonable grounds") und erscheint damit **kaum praktikabel.** Besser wäre es, die Betroffenen schlichtweg an den Kosten der Informationsbereitstellung zu beteiligen. **Der deutsche Vorschlag ist problematisch wegen Manipulationsrisiken.** Wenn überhaupt, sollten relevante Informationen auf vertrauenswürdigen Drittseiten vorgehalten werden. Die **Ausnahmen** (Weitergabe an Dritte; besondere Schutzbedürftigkeit) **zeichnen grundrechtliche Grenzen nach.** Diese Ausnahmen dürften also grundsätzlich zwingend sein.

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
Art. 3 Abs. 6	Einschränkung der kostenfreien Information über die Datenerhebung zu wiss. Zwecken	---	Die Regelung **schränkt die Möglichkeiten zur Datennutzung zu wissenschaftlichen Zwecken ein.** Sie enthält viele wertungsbedürftige Rechtsbegriffe („disproportionate effort"; „seriously impair"; „appropriate measures") und erscheint damit **kaum praktikabel.**. Besser wäre es, die Antragsteller schlichtweg an den Kosten der Informationsbereitstellung zu beteiligen.
Art. 3 Abs. 7	Begrenzung des Rechts, kein Gegenstand automatischer Datenverarbeitung (inkl. Profiling) zu sein (Art. 22 Abs. 1 DSGVO)	---	Die **Regelung beschränkt den Rechtsschutz.** Die trägt allerdings dem Umstand Rechnung, dass das Recht in der Praxis ohnehin nur auf dem Papier besteht. Sie erscheint **vertretbar.**
Art. 3 Abs. 8	Verlängerung der Fristen für die Meldung von Verletzungen; einheitliche Meldestelle und Übergangsregime; Formulare (Art. 33 DSGVO).	Nötige Vereinfachung der Meldung von Verletzungen; Ersetzung der 72-Stunden-Frist durch Frist v. 3 Arbeitstagen (Art. 33 DSGVO).	Die Regelungen des **Digital Omnibus erleichtern den Rechtsschutz** für Betroffene und **reduzieren tendenziell den behördlichen Aufwand.** Sie erscheinen daher sinnvoll.
Art. 3 Abs. 9	Präzisierung der Notwendigkeit und Anforderungen an Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)	---	Die Regelung sieht Vereinheitlichungen vor („common template"), aber verwendet wertungsbedürftige Begriffe hinsichtlich der festzulegenden Anforderungen. Im Interesse der Rechtsklarheit wäre es sinnvoll, wenn zumindest die **Branchen definiert** würden, in denen **Datenschutz-Folgenabschätzungen vorzunehmen** sind.
Art. 3 Abs. 10	Ermächtigung der EU-Kommission zu delegierter Rechtsetzung in Bezug auf Pseudonymisierung	Klarstellung: Anonymisierte Daten sind keine personenbezogenen Daten – aber: Anonymisierung ist Verarbeitung schutzwürdiger Daten.	Die Regelung im Digital Omnibus kann keine Rechtssicherheit schaffen: Der **Wegfall des Personenbezugs ist Tatsachenfrage. Die Regelung ist abzulehnen.** Der **deutsche Vorschlag** ist **dagegen zur Klarstellung des Begriffs „Datenverarbeitung" sinnvoll.**

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
---	---	In Art. 42 ff. DSGVO ist mehr Raum für Zertifizierungen zu geben; insb. durch Möglichkeit einer Hersteller-/Lieferantenzertifizierung, statt allein Verarbeiter haften zu lassen.	Der Digital Omnibus hat den **deutschen Vorschlag** nicht aufgegriffen. Der Vorschlag erscheint dennoch **sinnvoll.**
	---	Zusätzliche Regelungen zum Jugend-/Verbraucherschutz.	Die deutschen Vorschläge wurden im Digital Omnibus nicht aufgegriffen, erscheinen aber sinnvoll.
	---	Leitlinien für Datenschutz bei Archivierung.	
	---	Erleichterung der Datennutzung für F&E, wenn konkreter Nutzungszweck bei Datensammlung noch unbekannt.	

c) DSGVO und ePrivacy-RL (RL 2002/58/EG)

Vorschrift	Inhalt	Stellungnahme
Art. 3 Abs. 15; Art. 5 Abs. 2	Einschränkung der Platzierung von Cookies u.ä. auf den Nutzer-Endgeräten; insofern Neuregelung in Art. 88a, 88b DSGVO ausgehend vom bisherigen Art. 5 Abs. 3 RL 2002/58/EG.	Der Umstand, dass der **Digital Omnibus** nicht lediglich einen Opt-out für Tracking Cookies vorsieht, wie es zuvor in der Presse kolportiert wurde, ist zu begrüßen. **Tracking Cookies sind AGB- und datenschutzrechtlich problematisch.** Die Nutzung sollte auf Dauer zugunsten datenschutzfreundlicherer Technologien wie z. B. einer Entscheidungsmaske im Webbrowser (vgl. Art. 88b Abs. 6 DSGVO)

Vorschrift	Inhalt	Stellungnahme
		eingeschränkt werden. Dabei ist jedoch zu berücksichtigen, dass die zentrale Steuerung von Einwilligungen z. B. über einen Webbrowser **schwer zu implementieren** ist, weil Einwilligungen zweckgebunden erteilt werden. Die vorgeschlagenen Regelungen sollten deshalb überprüft werden, um einen fairen Ausgleich der Interessen von Vermittlungsdiensten, der Werbewirtschaft und der Verbraucher als Grundrechtsträger zu erreichen. Davon abgesehen sollte geprüft werden, **RL 2002/58/EG** zur Rechtsklarheit **insgesamt in die DSGVO zu integrieren.**
Art. 5 Abs. 1	Streichung von Art. 4 RL 2002/58/EG	Die zu streichende Vorschrift macht Vorgaben zur Sicherheit der Datenverarbeitung, dürfte aber durch Art. 25 DSGVO und RL 2022/2555 (NIS 2) überholt sein.

d) Digital Omnibus (Daten): Änderungen der NIS 2-Richtlinie

Vorschrift	Inhalt	Stellungnahme
Art. 6-9	Einheitliche Meldestelle für IT-Sicherheitsvorfälle (NIS2-RL, eIDAS-VO, Critical Entities-VO, DORA; DSGVO)	Die Regelungen des **Digital Omnibus erleichtern den Rechtsschutz** für Betroffene und **reduzieren tendenziell den behördlichen Aufwand.** Sie erscheinen daher sinnvoll.

e) Digital Omnibus on AI: Änderungen der KI-Verordnung

Vorschrift	Inhalt	Stellungnahme
---	Der Digital Omnibus on AI soll Umsetzungsschwierigkeiten ausräumen, die den effektiven Anwendungsbeginn der Hauptvorgaben der KI-VO gefährden könnten (COM(2025) 836 final, S. 2)	**Änderungen der KI-VO reichen nicht aus zur Schaffung von Rechtssicherheit und zur Verminderung bürokratischer Lasten.** Dafür wäre es insbesondere auch nötig, die Pflichten-/Haftungsverdoppelungen durch KI-VO einerseits und DSGVO/AVMD/DSA/RL über unlautere Geschäftspraktiken usw. andererseits in Hinblick auf die Generierung von KI-Outputs zu beseitigen. Außerdem werden die **relevanten Risiken** nach der gegenwärtigen KI-VO **fast alle als potenziell systemisch**

Vorschrift	Inhalt	Stellungnahme
		angesehen (Ausn.: Art. 51 ff.). Hier wäre zu differenzieren, um der Marktbedeutung des jeweiligen Einsatzes stärker Rechnung zu tragen.
---	Ankündigung von 13 weiteren Leitlinien zur Konkretisierung der KI-VO und zur Erleichterung ihrer Anwendung	**Eine Vielzahl ergänzender Leitlinien trägt nicht zur Rechtssicherheit und Anwendungserleichterung bei.** Die Notwendigkeit solcher Leitlinien indiziert einen missglückten Regelungsansatz der KI-VO. Die Leitlinien erhöhen den Umsetzungsaufwand zudem in einem Maße, das überhaupt nur durch größere Unternehmen zu bewältigen sein dürfte.
Art. 1 Abs. 1, 3	Erweiterung der Privilegierung von Kleinunternehmen (SMC neben SME).	**Mehrere Kategorien von Kleinunternehmen**, für die Sonderregelungen gelten, **vermindern** die **Rechtsklarheit**. Sie indizieren zudem, dass die Regeln der KI-VO auch nach dem Digital-Omnibus on AI die Wirtschaft übermäßig belasten. **Besser** wäre jedenfalls eine Ausnahme, die die Regulierung bei **geringem Umfang des Einsatzes von KI** unabhängig von der Unternehmensgröße zurücknimmt.
Art. 1 Abs. 4	Neufassung: Statt Anforderungen an KI-Kompetenz in Art. 4 KI-VO nun Unterstützung der KI-Bildung (AI literacy).	Die Regelung enthält nur eine vage Vorgabe, die nicht beachtet, dass einerseits die EU-Kommission keinen Bildungsauftrag und andererseits die Mitgliedstaaten ohnehin alle nötigen rechtlichen Kompetenzen haben, die KI-Bildung zu fördern (Art. 4 Abs. 1, Art. 5 Abs. 1, 2 EUV). Die Regelung hat **keinen erkennbaren Mehrwert.**
Art. 1 Abs. 5, 7	Berechtigung zur Verwendung personenbezogener Daten i.S. des Art. 9 DSGVO (s. Erw.-Grd. 6) zum KI-Training anstelle des bisherigen Art. 10 Abs. 5 KI-VO (Art. 4a KI-VO n.F.).	Die Regelung definiert **enge Bedingungen**, unter denen ein besondere Kategorien personenbezogener Daten für die Identifizierung von Verzerrungen („bias“) angenommen werden können. Sie stützt sich dabei auf wertungsbedürftige Begriffe („exceptionally process“; „suitable safeguards“). Die Regelung trägt weiter nur begrenzt zur Rechtsklarheit bei.
Art. 1 Abs. 6, 14	Neuregelung der Selbsteinschätzung als Betreiber von Nicht-Hochrisiko-KI (Art. 6 Abs. 4, 49 Abs. 2 KI-VO).	Die Neuregelung **reduziert den Verfahrensaufwand**, weil die Notwendigkeit der **Registrierung in einer EU-Datenbank entfällt.** Sie ist zu begrüßen.

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 8	Anforderungen an die technische Dokumentation von Hochrisiko-KI-Systemen (Art. 11 Abs. 1 UAbs. 2).	Die **Dokumentationsanforderungen** der KI-VO sind insgesamt problematisch: Sie sind sehr umfangreich und **weichen** zudem **vom allgemeinen Marktordnungsrecht ab**, wonach staatliche Stellen nur bei Missbräuchen und konkret drohenden Gefahren in den Markt eingreifen. Die Pflichten ermöglichen vielmehr eine engmaschige Überwachung wie z.B. im Finanzaufsichtsrecht, wo Systemgefährdungen abzuwenden sind. In Hinblick auf Hochrisiko-KI-Systeme ist die neugefasste Regelung samt der Begrenzungen für kleine Unternehmen aber **vertretbar**.
Art. 1 Abs. 9	Größenabhängige Anforderungen an Qualitätsmanagementsysteme (Neufassung Art. 17 Abs. 2 KI-VO)	Die **Regelung ist unklar**, da sie Anforderungen in Bezug auf ein seinerseits wertungsabhängiges Ziel definiert („respect the degree of rigour and the level of protection required to ensure the compliance“).
Art. 1 Abs. 10-15	Verschiedene Änderungen zu Notifizierungen, Konformitätsbewertungen und Praxisleitfäden (Art. 28-30, 43, 50 KI-VO).	Die Änderungen dienen der **Verwaltungsvereinfachung** und Verfahrensbeschleunigung. Insofern sind sie zu begrüßen.
Art. 1 Abs. 16	Überwachung von Praxisleitfäden: Teilhochzonung zur EU-Kommission (Art. 56 Abs. 6 KI-VO).	Die Vorschrift kann – sofern man diese für erforderlich hält – zu einer **effektiveren Aufsicht** beitragen und erhöht für die Marktteilnehmer die Übersichtlichkeit des Aufsichtssystems. Insofern ist sie zu begrüßen.
Art. 1 Abs. 17-19	Ermächtigung zu KI-Reallaboren auf EU-Ebene; weitere Regelungen zu KI-Reallaboren (Art. 57 Abs. 3a KI-VO n.F.).	Die Notwendigkeit von **KI-Reallaboren** (Art. 57 ff. KI-VO) ergibt sich allein daraus, dass KI in der EU einer weitgreifenden speziellen Überwachung unterworfen wird, mit Pflichten, die sich gleichwohl mit anderen Regelungen überschneiden (DSGVO, Verbraucherschutzrecht usw.). Insofern wird der Marktbedeutung der KI je nach Einsatzzweck zu wenig Rechnung getragen, wenn die Risiken grundsätzlich als (zumindest potenziell) systemische Risiken reguliert werden. Die Regelungen zu KI-Reallaboren **belegen** insofern die bestehende **Überregulierung.**
Art. 1 Abs. 20	Neuregelung zur Testung von Hochrisiko-KI-Systemen unter realen	Die Vorschrift steht geradezu **quer zum Regelungsansatz der KI-VO**, der KI-Systeme nach ihrem (potenziell systemischen) Risiko abgestuft reguliert und nur

Vorschrift	Inhalt	Stellungnahme
	Bedingungen außerhalb von Reallaboren (Art. 60a n.F. KI-VO).	Reallabore und diese bisher nur auf mitgliedstaatlicher, regionaler oder lokaler Ebene – d.h. bei begrenzten Auswirkungen im Fall der Risikorealisierung – vorsieht. Die Vorschrift ist zudem **schon jetzt durch die Entwicklung überholt:** In den letzten Jahren wurden KI-Modelle mit allgemeinem Verwendungszweck – wenngleich nicht definierte Hochrisiko-KI-Systeme – im Markt ausgerollt. Die weit verbreitete Nutzung, um die **Systeme unter realen Bedingungen zu testen und zu verbessern,** ist zwar weiterhin **nicht der gesetzliche Regelfall, aber praktisch ein wesentlicher Bestandteil** der Entwicklung bzw. Weiterentwicklung von KI-Systemen.
Art. 1 Abs. 21, 23	Ausnahmen von Vorgaben zu Qualitätsmanagementsystemen für Kleinunternehmen; Beratung (Art. 63 Abs. 1, Art. 70 Abs. 8 KI-VO n.F.).	Auch diese Regelungen sind **notwendig, weil die KI-VO** mit ihrem – ohne Differenzierungen auf potenzielle Systemrisiken ausgerichteten Ansatz – einzelfallabhängig **zu unverhältnismäßigen Anforderungen führen kann.** Anstelle einer Regelung abhängig von der Unternehmensgröße wäre es auch in diesem Kontext **besser**, die Regulierung bei **geringem Umfang des Einsatzes von KI unabhängig von der Unternehmensgröße** zurückzunehmen.
Art. 1 Abs. 25, 26	Zuständigkeitskonzentration für Marktüberwachung auf EU-Ebene; behördliche Kooperation (Art. 75, 77 KI-VO).	Die Änderungen dienen der **Verwaltungsvereinfachung** und können – sofern man diese für erforderlich hält – zu einer **effektiveren Aufsicht** beitragen. Insofern sind sie erneut zu begrüßen.
Art. 1 Abs. 27, 28	Verhaltenskodizes und Leitlinien für Kleinunternehmen (Art. 95, 96 Abs. 1 KI-VO)	Anstelle einer Regelung abhängig von der Unternehmensgröße sollte erneut der **Umfang des Einsatzes von KI-Technologie** im Unternehmen **maßgeblich** sein. Bei allen Unternehmen mit nur geringem KI-Einsatz ist die behördliche Unterstützung durch vereinfachende Leitlinien/Verhaltenskodizes gleichermaßen sinnvoll.
Art. 1 Abs. 29	Erweiterung der Regelungen zu Durchsetzung und Sanktionen auf zusätzliche Kleinunternehmen (Art. 99 KI-VO)	Die Vorschrift regelt weiter nur die **hoheitliche Durchsetzung** durch Behörden der Mitgliedstaaten. Hinsichtlich des zivilrechtlichen Rechtsschutzes ist sie offen. Dies verursacht **Rechtsunsicherheit bezüglich** der Frage, welche **Relevanz** die Anforderungen der KI-VO überhaupt **in Zivilrechtsverhältnissen** haben.

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 30, 31	Hinausschieben des Anwendungsbeginns der KI-VO (Art. 111, 113 KI-VO).	**Die Regelungen sind schon wegen des verfehlten Regulierungsansatzes der KI-VO zu begrüßen. Besser wäre es, die Verordnung würde insgesamt zurückgenommen und eine Neuregelung getroffen, die Risikoschutz und Innovationsförderung besser austariert.**

f) Verordnungsvorschlag über EU-Brieftaschen für Unternehmen (European Business Wallets)

Vorschrift	Inhalt	Stellungnahme
Art. 2	Anwendungsbereich: Bereitstellung und Annahme von Europ. Business Wallets und dafür geeignete Inhaber-Identfizierungsdaten; Einsatz von Europ. Business Wallets.	Die Europ. Business Wallet sollte nicht nur für Unternehmen, sondern auch für sondern auch für Datentransfers im Rahmen von Forschung und Entwicklung nutzbar sein.
Art. 6 Abs. 1	Funktionen von Europ. Business Wallets	Sinnvolle Regelung, insb. soweit auch eine Interaktion zwischen Europ. Business Wallets und European Digital Identity Wallets sicherzustellen ist. Allerdings sollten auch passende Identitätsfunktionen für Forschung und Entwicklung geschaffen werden.
Art. 7 Abs. 2	Anbieter von Europ. Bus. Wallets müssen Sitz in EU haben.	Die Regelung ist vertretbar, um die Rechtsdurchsetzung gegenüber den Anbietern und damit ihre Vertrauenswürdigkeit gewährleisten zu können.
Art. 9 Abs. 1	Nutzung von einem Unternehmen zugewiesenen einheitlichen Kennungen	Neben Unternehmen sollten auch Forschungsinstitutionen eine einheitliche Kennung erwerben können. Die Möglichkeit zum Identitätsmanagement über Europ. Business Wallets dürfte auch im Kontext von Forschung und Entwicklung außerhalb des Unternehmenskontexts relevant sein können.
Art. 9 Abs. 2	Zuweisung einer einheitlichen Kennung aufgrund einer Durchführungs-Rechtsakts	Neben den einheitlichen Kennungen, die von den Mitgliedstaaten nach Vorschriften zur Umsetzung der RL 2017/1132 vergeben werden, sollten auch durch

		internationale Organisationen entwickelte Kennungen wie z. B. der Legal Entity Identifier von GLEIF als unionsweit gültige „einheitliche Kennung“ anerkannt werden können.
Art. 10 Abs. 4	Verzeichnis für Inhaber von European Business Wallets	Außerdem sollte es ein frei einsehbares Verzeichnis geben, das Auskunft über Nutzungsbeschränkungen für Signaturen gibt, die unter Nutzung einer Europ. Business Wallet erteilt werden.

* * *

Policy Briefing: A Strategic Analysis of the EU's Digital Omnibus Package

Position Paper of the FCCR on the „Digital Omnibus“

R. Koch/T. Weck (authors)*
A. Diefenhardt/M. Jager/J. Redenius-Hövermann

1. Introduction: A Critical Juncture for EU Digital Policy

The European Commission's introduction of the "Digital Omnibus" package on November 19, 2025, represents a pivotal ***moment for European digital policy***. While the stated objective of simplifying regulation and thereby strengthening the competitiveness of the European economy is to be welcomed, the current regulatory approach – including the gradual changes proposed in the omnibus package – is not sufficient to meet the challenges of the global digital landscape. ***Regulation*** in recent years has become a “jungle” that is ***no longer comprehensible to those affected***, thereby excessively restricting the scope for self-determined behavior. The EU regulatory framework therefore needs more than just minor adjustments; it requires a fundamental ***conceptual realignment.***

The EU should go beyond individual changes and develop a new, data-friendly regulatory philosophy that also strictly protects fundamental rights. This reorientation is necessary to manage the complex ***interplay between two key political objectives:*** the Commission's efforts to strengthen the competitiveness of businesses and the efforts of the EU and the German government to expand digital sovereignty. It is crucial to recognize that these two objectives are not equivalent. A sober critique of the existing framework is the necessary first step toward developing a more coherent and effective strategy.

2. The Design Flaws of Current EU Digital Regulation

In order to chart a new course, it is essential to first understand the ***fundamental shortcomings of the EU's current approach*** to digital regulation. These shortcomings are not isolated problems, but interconnected difficulties that create significant legal uncertainty, stifle innovation, and ultimately undermine competitiveness and sovereignty. The prevailing framework is characterized by four main shortcomings:

- **Ambiguous and Conflicting Objectives:** Major regulations like the General Data Protection Regulation (GDPR) and the AI Act blend public tasks (e.g., fundamental rights protection) with private economic interests (e.g., promoting the free movement of data or supporting innovation). This fusion of disparate goals leads to vague mandates and significant implementation challenges, as regulators and businesses struggle to navigate contradictory priorities.
- **Insufficient Private Enforcement Mechanisms:** The regulatory framework heavily relies on state-led, administrative enforcement. In contrast, the mechanisms for private entities to seek recourse through civil courts remain largely ignored and uncertain. Even where the rules create rights for those affected, the mechanisms

* Roland Koch, former Minister President, is Professor of Management Practice, and Thomas Weck is Associate Professor at the Frankfurt Competence Centre for German and Global Regulation (FCCR) at the Frankfurt School of Finance and Management. The authors declare that the FCCR is funded by companies that have been or are involved in regulatory proceedings on the topics discussed here at the EU and/or national level, although it is independent of its funding partners.

for asserting legal remedies before civil courts in the Member States are inconsistent, which weakens the entire protection structure.

- **Suppression of innovation:** The EU regulatory model has become fundamentally risk-averse, preventively depriving companies of important risk management decisions. This creates a climate of uncertainty that inhibits investment in new digital business models. The fact is, however, that leading European companies have often produced innovations despite – and not because of – the existing regulatory environment.
- **Lack of future-proofing:** The regulatory model is reactive and hardly able to keep pace with technological developments. The initial failure of AI law to foresee the rise of large language models is a prime example of this shortcoming. The very necessity of the Digital Omnibus Package – created to revise several important laws passed only in the last five years – is an admission that the current approach is neither agile nor forward-looking or sustainable.

These foundational problems necessitate a move away from the current approach and toward a new, more coherent conceptual model for digital regulation.

3. A Counter-Proposal: Rebalancing Data Regulation by Addressee and Function

A more effective regulatory framework must move beyond simplistic data categories, such as "personal" versus "non-personal," to a more nuanced model. This model should be structured around two key dimensions: the ***actors involved*** in a data interaction (the addressee) and the ***context and purpose of the relevant interaction*** (the function). This would allow for targeted, proportionate, and logically consistent regulation in various areas of the digital economy.

a) State Access to Data for Sovereign Purposes

When the state accesses personal data for sovereign purposes that interfere with fundamental rights – such as law enforcement or national security – the primary concern remains the ***protection of individual liberties*** against state power. For this domain, the GDPR and national data protection laws provide a suitable and proven regulatory framework. They strike a balance between enabling legitimate state tasks and protecting the rights of individuals. Existing rules should remain unaffected regarding state measures. Nevertheless, efficiency gains could be achieved if other public administration bodies were allowed to ***use existing data*** to fulfill their legal tasks. This should apply in any case where duplicate data collection can be avoided and no fundamental protection interests risk to be violated.

b) Data Use in Business-to-Consumer (B2C) Relationships

In business transactions between companies and consumers, the regulatory challenge is different. Here, consumers are not subject to state control, but exercise their freedom of contract. The core problem is the ***structural imbalance of bargaining power*** between the two parties. The current consent practice under the GDPR (Art. 6(1)(a)) is ineffective in this context; it does not take into account the considerable ***information deficit on the part of consumers*** and ultimately leads to legal responsibility being shifted onto them through mechanisms such as cookie banners. Centralized control of consent, e.g., via a web browser, is difficult to implement because consent is granted for specific purposes.

A more effective approach would be to move away from the consent model altogether and instead base consumer protection on solid contract and consumer law, such as ***standardized terms and conditions*** (civil law; cf. the current P2B Regulation). In addition, ***supervision*** of cross-border online services should be consolidated nationally ***in a single authority*** (such as the German Federal Network Agency) to ensure uniform enforcement. In addition, the development of model declaratory actions should be monitored in order to readjust ***civil law remedies*** for consumers if necessary.

c) Data Exchange in Business-to-Business (B2B) Relationships

The ***existing regulation*** of B2B data exchange ***remains inadequate.*** It does not address the key challenges of the market consistently enough, namely ensuring technical interoperability, overcoming information asymmetries, and striking a balance between data access and the legitimate protection of trade secrets. The European Health Data Space (EHDS) offers a ***more practical model*** than the Data Act, striking a better balance between data access and intellectual property protection.[5]

d) Data Use in Research and Development (R&D)

The ability to use and exchange data for research and development is a cornerstone of competitiveness. However, the current European landscape is too fragmented and restrictive. This leads to data remaining completely unused or to unnecessary multiple surveys (contrary to the once-only principle). A more efficient approach is needed to unlock innovation potential. The most important reforms should include:

- **Consolidating and simplifying** the multitude of data access rules that apply to public bodies under directives such as the Public Sector Information (PSI) Directive, INSPIRE, and others.
- **In Germany,** government agencies are permitted to use data within their remit in compliance with data protection laws. The scope of the upcoming Research Data Act will be expanded to allow access to data from all departmental research institutions.
- **At EU level,** concerted efforts are being made to reduce the fragmentation of data access standards and create a more coherent framework for researchers.

Further, the instruments of the ***Data Governance Act (DGA) are of limited use*** for R&D. The assumption that trust in data use arises primarily through the regulation of intermediaries falls short. What is more important is whether the data source is trustworthy and that data use is delimited in a legally secure fashion. In this regard, the ***"European Business Wallet"*** proposed in the Digital Omnibus ***appears more promising.*** However, this would require research institutions to be able to obtain a uniform identifier and the establishment of a freely accessible directory providing information on usage restrictions for EBW signatures.

e) Regulation of Artificial Intelligence (AI)

The fundamental approach of the AI Act is deeply flawed. The Act creates an ***additional layer of regulation*** on top of existing product safety and liability laws and establishes a

[5] The strict regulation in Sec. 393 of the German Social Code, Book V (SGB V) can be used as a supplement for questions regarding cloud use.

burdensome, surveillance-like compliance system that is ***unsuitable for a fast-moving technology sector.***

The core problem with the law is that it focuses on the ***risks of AI outputs*** and their generation ***without providing legal certainty for the inputs*** that are crucial for AI development and innovation—in particular, the use of personal data, copyrighted content, and trade secrets for training models. This places innovators in a legal gray area. The AI Act thus ***sends*** an extremely ***negative signal to the market*** and directly hinders the EU's goals of strengthening competitiveness and digital sovereignty. The law must be fundamentally revised to strike a sustainable balance between risk management and innovation, or even repealed entirely.

4. Reclaiming Digital Sovereignty as a Core State Interest

"Digital sovereignty" has become a central objective of EU and German policy, but its meaning is often misunderstood. It is critical to draw a clear distinction: ***digital sovereignty is a state interest,*** concerned with maintaining control over critical digital infrastructure and state functions. ***Competitiveness is a corporate interest***, pursued by businesses within a given market framework. The German government's conflation of these two concepts is a fundamental error that leads to misguided policy.

From the perspective of digital sovereignty, complex regulations such as the ***Digital Markets Act*** (DMA) ***and the Digital Services Act*** (DSA) are not a sign of European resilience, but rather a ***symptom of long-standing political failure:*** For years, politicians failed to recognize or address the core problem of inadequate law enforcement in the areas of competition and platforms – proceedings against large US platforms sometimes took a decade. Additional behavioral obligations, such as those now included in the DMA and DSA, which in turn must be enforced, do not remedy the actual ***enforcement deficit.*** At the same time, these regulations are largely ***symbolic politics*** because they do not change anything about key structural challenges – in particular, business models based on personal data and the lack of effectiveness of GDPR consent. Instead, the DMA even adopts the flawed consent logic and thus falls short of effective consumer protection.

A ***genuine strategy*** for digital sovereignty must be proactive and structural. It requires a focus on four key measures:

1. **Decentralize Critical Digital Infrastructure:** Reduce dependency on single providers by promoting decentralized architectures, especially for government services and essential economic sectors like finance and energy.
2. **Promote Open Protocols and Standards:** Foster the use of open-source technologies and interoperable standards to break down walled gardens and reduce vendor lock-in.
3. **Strengthen Effective Legal Enforcement:** Prioritize simple, clear rules that can be enforced quickly and effectively. This requires a well-resourced judicial system and a clear focus on neutralizing violations rather than merely imposing fines.
4. **Increase Political Momentum:** Transparently disclose the ongoing costs and strategic risks arising from dependencies on foreign digital services and infrastructures (e.g., due to license restrictions).

This strategic reorientation provides the foundation for the specific policy recommendations that follow.

5. Analysis and Recommendations for the Digital Omnibus Package

This section offers a targeted critique of the specific legislative proposals on data and AI within the Digital Omnibus Package. While some of the proposed changes are beneficial, many either reinforce the flawed regulatory philosophy outlined above or create new problems that will further complicate the legal landscape.

a) Proposed Amendments to the Data Act

The amendments to the Data Act present a ***mixed picture:*** they combine sensible consolidation with the preservation of failed concepts.

- **Positive:** Consolidating various related legal acts (such as the regulation on the free flow of non-personal data, the Data Governance Act, and the Data Act) into a single instrument is a sensible step toward simplification. Similarly, the introduction of measures to protect public data from uncontrolled access by third countries is a welcome step towards strengthening resilience.
- **Negative:** The decision to adopt the failed DGA rules on data intermediaries and data altruism is a serious mistake. These provisions have proven ineffective and alien to the market and should be deleted, not integrated. Furthermore, the new rules on the protection of trade secrets are impractical, and the creation of multiple, overlapping definitions for small and medium-sized enterprises leads to excessive complexity.

b) Proposed amendments to the GDPR and the ePrivacy Directive

The proposed amendments to the GDPR risk creating ***more uncertainty*** than they eliminate.

- The proposal to introduce a new ***"subjective" definition*** of personal data based on whether a specific body can identify a person establishes a situation-dependent standard that is unsuitable for the protection of fundamental rights. It would create legal uncertainty and immense difficulties in proving cases in legal disputes.
- The idea of a ***"three-tier model"*** that applies different rules depending on the size of the company is to be rejected. The risk arises from the nature of the processing activity, not from the size of the company carrying it out. The principle must be: "Same risk, same regulation."
- The new provisions clarifying the use of personal data in ***AI training*** are insufficient. They do not offer innovators the necessary legal certainty and potentially weaken the protection of fundamental rights without strengthening the position of data subjects accordingly.

c) Regulation of digital identities ("European Omnibus Wallet")

The introduction of a digital corporate identity is to be welcomed. The proposed regulation presented in the "Digital Omnibus" package is limited to what is necessary and involves little bureaucratic burden. However, it would be desirable for ***identifiers developed by international organizations*** to also be recognized as "uniform identifiers" throughout the EU. In addition, steps should be taken to ensure that ***research institutions*** can also obtain a uniform identifier under EU law and that a ***freely accessible directory*** is set up to provide information ***on restrictions on the use of EBW signatures.***

At the ***national level***, there are initiatives – such as the establishment of a basic register for company data at the Federal Statistical Office – that should also be taken into account in the design of new EU legislation in the interest of more comprehensive and consistent regulation of digital identities.

d) Proposed amendments to the AI Act

The "Digital Omnibus on AI" offers only ***superficial solutions*** that do not remedy the fundamental design flaws of the AI Act.

The fact that the Commission has announced the need for ***13 additional guidelines*** to clarify the law is a tacit ***admission of a failed regulatory approach.*** These guidelines will only increase the compliance burden on businesses.

The creation of ***special privileges*** for different categories of small businesses is ***further evidence*** that the ***regulation is too burdensome for everyone.*** Instead of creating complex exemptions, the basic rules should be proportionate and practical.

The proposals do not address the ***many core problems of the AI Act:*** duplicate liability rules, significant legal uncertainty regarding training data, and the chilling effect on innovation. While ***delaying the application*** of the law is a ***welcome tactical move,*** it does not replace the necessary strategic overhaul.

6. Conclusion: Key recommendations for a revised regulatory framework

The European Union is at a ***crossroads.*** To secure its digital future, it must shift from its current complex, risk-averse, and burdensome regulatory policy to a clear, principle-based framework that enables innovation, promotes competition, and effectively protects citizens. The Digital Omnibus package offers an opportunity to initiate this change, but only if it is accompanied by a more profound paradigm shift.

The following ***overarching recommendations*** summarize the key measures required for a successful regulatory realignment:

- **The GDPR should be refocused on its core purpose:** protecting fundamental rights in interactions between the state and citizens. In commercial transactions, specific, targeted consumer and contract laws should be used to eliminate power imbalances.
- **Promote B2B data exchange** by abolishing failed DGA models for data transfer and instead focusing on practice-oriented, industry-led standards for interoperability and the effective protection of trade secrets.
- **Data use in research and development should be significantly simplified and harmonized.** In Germany, state institutions should be given greater scope to use existing data within the framework of their legal mandate, and the scope of the planned Research Data Act should be extended to all departmental research institutions. At the EU level, coordinated initiatives are needed to reduce existing fragmentation and provide researchers with coherent, reliable access to data.
- **The AI Act should be fundamentally revised** to eliminate regulatory duplication with existing liability laws, create clear legal certainty for the use of training data, and align compliance burdens with demonstrable systemic risks, not arbitrary parameters such as company size.

- **Pursue digital sovereignty as a national strategy** by focusing on concrete, structural measures—such as promoting decentralized infrastructure, open standards, and the rapid enforcement of existing laws – rather than creating new layers of complex and often symbolic regulation.

* * *

Appendix to the position paper: Statement on the individual provisions in the Digital Omnibus Package

On November 19, 2025, the European Commission presented its seventh omnibus package and is seeking comments on it until March 13, 2026. This position paper comments on the proposed regulations contained therein for a "Digital Omnibus" on data, a "Digital Omnibus on AI," and a proposed regulation on European Business Wallets.[6] The proposed regulations are currently only available in English.

e) Digital Omnibus (Data): Amendments to the Data Act

Regulation	Content	Opinion
---	Integration of FFDR, DGA, Data Act, Open Data Directive in the Data Act	**Integration is generally useful**, as the system is currently unclear and there are overlaps between legal acts. However, converting the Open Data Directive into **regulatory law** is not without its problems: The Directive is about control over public sector information, its availability and reuse (Rec. 16), which may be **relevant** to **the internal and external security of Member States**. **As an alternative** to integrating the rules on data reuse in the Data Act, the **DGA provisions** on this could also be **integrated into the Open Data Directive**, leaving Member States room for maneuver in their implementation.
---	Criminal data retention is regulated separately	This makes sense, as it is **a separate issue:** access to personal data for security purposes.
Art. 1(2)(d)	Inclusion of the DGA provisions on data intermediation services/data altruism in the Data Act	The rules have **not proven effective** and should be removed without replacement. A subsequent evaluation (Art. 1(26) = Art. 49 Data Act, new version) offers no discernible added value.
Art. 1(2)(e)	Definition of 'medium-sized enterprise'/'small mid-cap'	**Multiple categories of small businesses** subject to special regulations **reduce legal clarity**. They also indicate that the rules of the Digital Omnibus continue to place an excessive burden on the economy.

[6] COM(2025) 836 final and COM(2025) 837 final.

Regulation	Content	Opinion
Art. 1(3), (4)	Introduction of a right of refusal for trade secret holders regarding data access (Art. 4(8), Art. 5(11) Data Act)	The obligation of data recipients to protect the **trade secrets** of the original data owner leads to **risks** for the data owner **that are difficult to assess**. In this respect, the agreement between the product user and the recipient constitutes a contract at the expense of third parties (the original data owner). **Legal uncertainty** due to the combination **of legal terms that are highly subject to interpretation** ("exceptional circumstances," "highly likely," "serious economic damage," "on a case-by-case basis"). **Data access** should be structured **in accordance with** the Data Act **and the EHDS Regulation**. The regulatory approach of the Data Act is fundamentally flawed.
Art. 1 (6)-(14)	Limiting data access for public authorities to cases of "public emergency" instead of "exceptional need"	This restriction **reduces the** potential **burden** on companies and appears **unproblematic** in view of the goal of competitiveness.
Art. 1 (15)	Regulations on cloud switching (Art. 23 ff. Data Act) are simplified (new Art. 31 (1a), (1b) Data Act).	**Regulatory approach is to be questioned:** In addition to storage, there is also demand for very specific services → The need for isolated switching rules in Art. 23 ff. Data Act remains unclear overall. Migration is made more difficult not so much by incompatible functionalities as by incompatible software architectures/interfaces and data formats.
Art. 1(16)	Reuse of public data subject to the proviso that access by third countries can be prevented (Article 32 Data Act)	This makes sense in order **to strengthen resilience in the EU's external relations.** **However, the wording of the provision is unclear:** references to other provisions, legal terms requiring interpretation ("minimum amount of data permissible"; "reasonable interpretation").
Art. 1(17)	Deletion of the provision on smart contracts (Art. 36 Data Act)	Makes sense as the provision is impracticable and leads to legal uncertainty (according to the EU Commission itself; COM(2025) 837 final, p. 5 and recital 16).

Regulation	Content	Opinion
Art. 1(18)	Adoption of DGA provisions on data intermediation services and data altruism	The **provisions** have **not proven effective** and, instead of the planned streamlining within the Data Act (Art. 32a ff. new version), would be better removed without replacement. A subsequent evaluation (Art. 1(26) = Art. 49 Data Act new version) offers no discernible added value.
Art. 1 para. 18	Adoption of DGA regulations on the reuse of public data	The **adoption of these provisions (Art. 32i ff. Data Act, new version) makes sense**. This will create uniform standards for public data. The **consolidation with the provisions of the Open Data Directive (Art. 32n ff. Data Act, new version)** also makes sense, but is not without problems due to the importance of the data concerned for the sovereign information management of the Member States (see above, line 1). In particular, the provisions on the **identification of "high-value datasets"** (Art. 14 Directive (EU) 2019/1024; Art. 32v Data Act, new version) also contain many legal terms that require interpretation. As a result, they contribute **little** to **legal certainty**. In any case, it would be better to comprehensively standardize the rules for public data, insofar as it can be used for statistical or scientific purposes: • Data access has so far been regulated in a fragmented manner (see also Directive 2007/2/EC; Directive 2003/4/EC); • Duplications in special regimes, such as for health data (Regulation 2025/327 – EHDS), should be reduced for greater legal clarity (e.g., regarding rights/documentation/compliance requirements).
Art. 1(18)	Inclusion of the FFDR data localization ban in the Data Act	The incorporation of **the data localization ban (Art. 32h Data Act, new version) is justifiable**, but its practical significance is likely to be limited. The removal of the FFDR provisions on codes of conduct for data sharing is justifiable due to their limited regulatory effect.

Regulation	Content	Opinion
		However, in the interests of **promoting interoperability and uniform** data formats in general, the **scope of Art. 33 ff. of** the Data Act should be **extended beyond European data spaces**.

f) Digital Omnibus (Data): Amendments to the General Data Protection Regulation (GDPR)

In anticipation of the presentation of the Digital Omnibus, Germany had submitted proposals to the European Commission for simplifying the GDPR. This **"German proposal for simplification of the GDPR"** was published by Netzpolitik.org on October 23, 2025, and was incorporated into the Digital Omnibus package following the impact assessment. It is therefore also taken into account in the following comments.

GDPR

Regulation	Content	German position	Statement
---	Summary of GDPR and e-Privacy Directive 2002/58/EC.	---	Makes generally sense.
---	---	Call for a better balance between the protected interests concerned: • General personal rights of those affected by data processing • Economic freedom/ freedom of science of data processors	Additional considerations: • Public interest in data use for the fulfillment of public interest obligations • Digital sovereignty (resilience) vis-à-vis non-EU countries; but also limits for EU industrial policy (Art. 173 TFEU)

Regulation	Content	German position	Statement
Art. 3(1)	Revised definition of "personal data" (Art. 4 GDPR):	---	Introduction of a "subjective approach" that limits the scope of the law to situations in which a person can be identified by a specific company. The new provision implements ECJ C-413/23 P – *EDSB*. However, it carries the risk that **companies** will **strategically** exclude themselves from **collecting** personal **data**, but at the same time ensure that they provide their business partners with data that may be personal (without the data subjects having a direct relationship with these other companies). In addition, the assessment of data collection under the GDPR is made more difficult by terms that are highly open to interpretation ("not [...] personal [...] where that entity cannot identify the natural person [...] taking into account the means reasonably likely to be used by that entity"). In this respect, the new provision is likely to cause **considerable difficulties** in terms of evidence in disputes. It would be **better to align** the **scope of the GDPR more closely with the relevant fundamental rights issues** and, in particular, to differentiate between government and company data processing.
---	---	Examination of **a 3-layer model** (see, for example, Wendehorst): Extensive obligations for large companies, regular obligations, reduced obligations/exceptions for SMEs and non-economic activities	**To be rejected: The need for protection of data subjects does not depend on the size of the processing company, but on the risks of processing** ("same risk – same regulation"). Data protection requirements must also be limited to what is necessary in order to be compatible with entrepreneurial freedom (Art. 16 CFR). The necessary requirements can usually be implemented better by large companies than by smaller ones. Large companies have more resources for this.

Regulation	Content	German position	Statement
			It would be **better to align** the **scope of the GDPR more closely with the relevant fundamental rights issues** and, in particular, to differentiate between government and company data processing.
Art. 3(2)	Feedback of the principle of purpose limitation (Art. 5(1)(b) GDPR) to the purpose limitation rule in Art. 6(4) GDPR	---	Clarification makes sense.
Recital 30 f.	Data use for AI training should be recognized as a "legitimate interest."	Safe harbor for setting up AI systems in compliance with the GDPR.	**The Digital Omnibus refrains from amending the wording of the law (Art. 6(1)(f) GDPR). The regulation is therefore insufficient to create legal certainty.** This would also require rules on the use of copyright-protected content and trade secrets for the training of AI models.
Art. 3(3)	Restriction of protection for specially protected data (Art. 9 GDPR) for cases involving the training of AI models and the processing of biometric data for identity verification	Access to specially protected data (Art. 9 GDPR) should (only) be simplified in emergency situations (e.g., pandemic).	The **exemption** of the use **of** specially protected data **for AI training purposes** serves to protect entrepreneurial freedom (Art. 16 CFR) in the development of innovative AI products, but **severely restricts the protection of fundamental rights for data subjects.** The **requirement** that appropriate **technical and organizational measures** must be taken to minimize the collection of relevant data and to protect such data (Art. 9(5) GDPR, new version) **is not sufficient.** In addition, the legal position of data subjects would have to be strengthened, e.g., by a presumption rule with regard to damages. Compatibility with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union is therefore doubtful. With this provision, the EU legislator is failing to fulfill its **duty to protect** consumers from **the risk of exploitation**.

Regulation	Content	German position	Statement
			The **use of biometric data** should be limited to cases where the data is under **the sole control of the person concerned**. The provision appears reasonable. The **German proposal is sensible.**
Article 3(4)	Restriction of free information about data collection from the data subject or elsewhere (Article 12(5) GDPR).	Restriction of abusive requests for information (Art. 15, 57 GDPR).	The **Digital Omnibus** regulation restricts the right to free information for abusive requests for information, with the burden of proof for abuse lying with the data processor. The **regulation appears reasonable.** The German proposals, on the other hand, are too cumbersome.
Art. 3(5)	Limitation of information about data collection from the data subject (Art. 13(4) GDPR) within the framework of existing legal relationships and where information is already available to the data subject.	Reduction of information obligations (Art. 13 GDPR): Companies should only provide relevant information on their own websites.	**The Digital Omnibus rule set** restricts the right to information in cases where the data subjects do not need the information to exercise their rights. The regulation contains many legal terms that require interpretation ("clear and circumscribed relationship"; "activity that is not data-intensive"; "reasonable grounds") and therefore seems **hardly practicable.** It would be better to simply have the data subjects contribute to the costs of providing the information. **The German proposal is problematic because of the risk of manipulation.** If anything, relevant information should be provided on trustworthy third-party websites. The **exceptions** (disclosure to third parties; special vulnerability) **outline fundamental rights limits.** These exceptions should therefore be mandatory in principle.
Art. 3(6)	Restriction of free information about data collection for scientific purposes	---	The regulation **restricts the possibilities for using data for scientific purposes.** It contains many legal terms that require interpretation ("disproportionate effort"; "seriously impair"; "appropriate measures") and therefore appears to **be impractical**. It would be

Regulation	Content	German position	Statement
			better to simply require applicants to contribute to the costs of providing the information.
Art. 3(7)	Limitation of the right not to be subject to automated data processing (including profiling) (Art. 22(1) GDPR)	---	The **provision restricts legal protection.** However, it takes into account the fact that in practice, the right exists only on paper anyway. It appears **reasonable.**
Art. 3(8)	Extension of the deadlines for reporting breaches; uniform reporting office and transitional regime; forms (Art. 33 GDPR).	Necessary simplification of the reporting of breaches; replacement of the 72-hour deadline with a deadline of 3 working days (Art. 33 GDPR).	The provisions of **the Digital Omnibus facilitate legal protection** for data subjects and **tend to reduce the administrative burden.** Thus, they appear reasonable.
Art. 3(9)	Clarification of the necessity and requirements for data protection impact assessments (Art. 35 GDPR)	---	The provision provides for standardization ("common template"), but uses terms that require interpretation with regard to the requirements to be specified. In the interest of legal clarity, it would be useful if at least the **sectors** in which **data protection impact assessments** are to be **carried out** were **defined**.
Art. 3(10)	Authorization of the EU Commission to adopt delegated legislation with regard to pseudonymization	Clarification: Anonymized data are not personal data – but anonymization is the processing of data worthy of protection.	The provision in the Digital Omnibus cannot create legal certainty: the **removal of the personal reference is a question of fact. The provision should be rejected.** The **German proposal, on the other hand**, is **useful for clarifying the term "data processing."**
---	---	In Art. 42 ff. GDPR, more scope should be given to certifications, in particular through the possibility of manufacturer/supplier	The Digital Omnibus has not taken up the **German proposal**. Nevertheless, the proposal appears to be **sensible.**

Regulation	Content	German position	Statement
		certification, rather than holding processors solely liable.	
	---	Additional regulations on youth/consumer protection.	The German proposals were not taken up in the Digital Omnibus, but appear sensible.
	---	Guidelines for data protection in archiving.	
	---	Facilitation of data use for R&D if the specific purpose of use is not yet known at the time of data collection.	

g) GDPR and ePrivacy Directive (Directive 2002/58/EC)

Regulation	Content	Opinion
Art. 3(15); Art. 5(2)	Restriction on the placement of cookies and similar items on users' end devices; in this respect, new rules in Articles 88a and 88b GDPR are based on the previous Article 5(3) of Directive 2002/58/EC.	The fact that the **Digital Omnibus** does not merely provide for an opt-out for tracking cookies, as previously reported in the press, is to be welcomed. **Tracking cookies are problematic in terms of general terms and conditions and data protection law.** Their use should be restricted in the long term in favor of more privacy-friendly technologies, such as a decision screen in the web browser (cf. Art. 88b (6) GDPR) . However, it should be noted that central control of consent, e.g., via a web browser, is **difficult to implement** because consent is granted for specific purposes. The proposed regulations should therefore be reviewed in order to achieve a fair balance between the interests of intermediary services, the advertising industry, and consumers as holders of fundamental rights.

Regulation	Content	Opinion
		Apart from that, consideration should be given **to integrating Directive 2002/58/EC into the GDPR as a whole** for the sake of legal clarity**.**
Art. 5(1)	Deletion of Art. 4 Directive 2002/58/EC	The provision to be deleted sets out requirements for the security of data processing, but is likely to be superseded by Article 25 GDPR and Directive 2022/2555 (NIS 2).

h) Digital Omnibus (Data): Amendments to the NIS 2 Directive

Provision	Content	Opinion
Articles 6-9	Single point of contact for IT security incidents (NIS2 Directive, eIDAS Regulation, Critical Entities Regulation, DORA; GDPR)	The provisions of **the Digital Omnibus facilitate legal protection** for those affected and **tend to reduce the administrative burden.** They therefore appear reasonable.

i) Digital Omnibus on AI: Amendments to the AI Regulation

Regulation	Content	Opinion
---	The Digital Omnibus on AI is intended to remove implementation difficulties that could jeopardize the effective start of application of the main provisions of the AI Regulation (COM(2025) 836 final, p. 2).	**Amendments to the AI Regulation are not sufficient to create legal certainty and reduce bureaucratic burdens.** To achieve this, it would be necessary, in particular, to eliminate the duplication of obligations/liabilities under the AI Regulation on the one hand and the GDPR/AVMD/DSA/Directive on unfair commercial practices, etc. on the other in relation to the generation of AI outputs. Furthermore, under the current AI Regulation**, almost all relevant risks** are considered **potentially systemic** (except for Art. 51 ff.). A distinction should be made here in order to take greater account of the market significance of the respective application.

Regulation	Content	Opinion
---	Announcement of 13 further guidelines to clarify the AI Regulation and facilitate its application	**A multitude of supplementary guidelines does not contribute to legal certainty and ease of application.** The need for such guidelines indicates a failed regulatory approach in the AI Regulation. The guidelines also increase the implementation effort to an extent that is likely to be manageable only by larger companies.
Art. 1 (1), (3)	Extension of privileges for small businesses (SMC in addition to SME).	**Multiple categories of small** businesses subject to special regulations **reduce legal clarity**. They also indicate that the rules of the AI Regulation continue to place an excessive burden on the economy even after the Digital Omnibus on AI. In any case, it would be **better** to have an exception that removes the regulation for **small-scale use of AI**, regardless of the size of the company.
Art. 1 (4)	Revised version: Instead of requirements for AI competence in Art. 4 AI Regulation, now support for AI education (AI literacy).	The provision contains only a vague requirement that fails to take into account that, on the one hand, the EU Commission has no educational mandate and, on the other hand, the Member States already have all the necessary legal powers to promote AI education (Art. 4(1), Art. 5(1), (2) TEU)**.** The provision has **no discernible added value.**
Article 1(5), (7)	Authorization to use personal data within the meaning of Art. 9 GDPR (see Recital 6) for AI training instead of the previous Art. 10(5) AI Regulation (Art. 4a AI Regulation, new version).	The provision defines **narrow conditions** under which special categories of personal data may be accepted for the identification of bias. It is based on terms that require interpretation ("exceptionally process"; "suitable safeguards"). The provision contributes only to a limited extent to additional legal clarity.
Art. 1(6), 14	New regulation on self-assessment as an operator of non-high-risk AI (Art. 6(4), 49(2) AI Regulation).	The new provision **reduces the procedural burden** because **it eliminates** the need for **registration in an EU database.** It is to be welcomed.
Art. 1(8)	Requirements for the technical documentation of high-risk AI systems (Art. 11(1) subparagraph 2).	The **documentation requirements** of the AI Regulation are problematic overall: they are very extensive and also **deviate from general market regulation law** , according to which government agencies only intervene in the market in cases of abuse and concrete imminent danger. Rather, the obligations enable close monitoring, as is the case, for example, in financial supervisory law, where systemic risks

Regulation	Content	Opinion
		must be averted. With regard to high-risk AI systems, however, the revised provision, including the limitations for small businesses, is **reasonable**.
Art. 1 (9)	Size-dependent requirements for quality management systems (revised Art. 17(2) AI Regulation)	The **regulation is unclear** because it defines requirements in relation to a goal that is itself value-dependent ("respect the degree of rigour and the level of protection required to ensure compliance").
Art. 1(10)-(15)	Various amendments to notifications, conformity assessments, and practical guidelines (Articles 28-30, 43, 50 of the AI Regulation).	The changes serve to **simplify administration** and speed up procedures. In this respect, they are to be welcomed.
Art. 1(16)	Monitoring of guidance documents: sub-delegation to the EU Commission (Art. 56(6) CRR).	The provision can contribute to **more effective supervision**, if deemed necessary, and increases the transparency of the supervisory system for market participants. In this respect, it is to be welcomed.
Art. 1 (17)-(19)	Authorization for AI real-world laboratories at EU level; further regulations on AI real-world laboratories (Art. 57(3a) AI Regulation, new version).	The need for **AI regulatory sandboxes** (Art. 57 et seq. AI Regulation) arises solely from the fact that AI in the EU is subject to extensive special monitoring, with obligations that nevertheless overlap with other rules (GDPR, consumer protection law, etc.). In this respect, the market significance of AI is not sufficiently taken into account, depending on the intended use, if the risks are regulated as (at least potentially) systemic risks. The regulations on AI regulatory sandboxes thus **demonstrate** the existing **overregulation.**
Art. 1 (20)	New regulation on testing high-risk AI systems under real conditions outside regulatory sandboxes (Art. 60a new version of the AI Regulation).	The provision is **at odds with the regulatory approach of the AI Regulation**, which regulates AI systems according to their (potentially systemic) risk and only provides for regulatory sandboxes, and these only at the Member State, regional, or local level—i.e., with limited impact in the event of risk realization. The provision is also **already outdated due to developments:** In recent years, AI models for general use – albeit not defined high-risk AI systems – have been rolled out on the market. Although widespread use **to test and improve systems under**

Regulation	Content	Opinion
		real-world conditions is still **not the legal norm, it is in practice an essential part** of the development and refinement of AI systems.
Art. 1 (21), (23)	Exceptions to quality management system requirements for small businesses; consultation (Art. 63(1), Art. 70(8) AI Regulation, new version).	These provisions are again **necessary because the AI Regulation**, with its approach that does not differentiate between potential system risks, **can lead to disproportionate requirements** in individual cases**.** Instead of a rule based on company size, it would also be **better** in this context to withdraw the regulation for **small-scale use of AI**, **regardless of company size**.
Art. 1(25), (26)	Concentration of responsibilities for market surveillance at EU level; cooperation between authorities (Art. 75, 77 AI Regulation).	The amendments serve to **simplify** administration and, if deemed necessary, can contribute to **more effective supervision**. In this respect, they are again to be welcomed.
Art. 1(27), (28)	Codes of conduct and guidelines for small businesses (Art. 95, 96(1) CSR)	Instead of a regulation based on company size, the **extent to which AI technology is used** in the company should once again be **the decisive factor**. For all companies with only limited use of AI, regulatory support in the form of simplified guidelines/codes of conduct is equally useful.
Art. 1(29)	Extension of enforcement and sanction rules to additional small businesses (Art. 99 AI Regulation)	The provision continues to regulate only **sovereign enforcement** by authorities of the Member States. It is open with regard to civil law protection. This causes **legal uncertainty as** to **the relevance** of the requirements of the AI Regulation **in civil law relationships**.
Art. 1 (30), (31)	Postponement of the date of application of the AI Regulation (Art. 111, 113 AI Regulation).	**The provisions are to be welcomed if only because of the AI Regulation's misguided regulatory approach. It would be better if the regulation were withdrawn altogether and new provisions adopted that strike a better balance between risk protection and the promotion of innovation.**

j) Proposed regulation on EU wallets for businesses (European Business Wallets)

Regulation	Content	Opinion
Art. 2	Scope: Provision and acceptance of European Business Wallets and suitable holder identification data; use of European Business Wallets.	The European Business Wallet should be usable not only for companies, but also for data transfers in the context of research and development.
Art. 6 (1)	Functions of European Business Wallets	The provision makes sense, especially insofar as interaction between European Business Wallets and European Digital Identity Wallets must be ensured. However, suitable identity functions should also be created for research and development.
Art. 7(2)	Providers of European Business Wallets must be based in the EU.	The provision is reasonable in order to ensure legal enforcement vis-à-vis providers and thus their trustworthiness.
Art. 9(1)	Use of uniform identifiers assigned by a company	In addition to companies, research institutions should also be able to acquire a uniform identifier. The possibility of identity management via European business wallets may additionally be relevant in the context of research and development outside an entrepreneurial context.
Art. 9(2)	Assignment of a unique identifier on the basis of an implementing act	In addition to the unique identifiers assigned by Member States in accordance with the provisions implementing Directive 2017/1132, identifiers developed by international organizations such as the GLEIF Legal Entity Identifier should also be recognized as "unique identifiers" valid throughout the Union.
Art. 10(4)	Directory of European Business Wallet holders	In addition, there should be a freely accessible register providing information on restrictions on the use of signatures issued using a European Business Wallet.

* * *