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

23.01.2026

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.

* * *