



MASSNAHMEN FÜR **MEHR DIGITALE SOUVERÄNITÄT**

cum ratione gGmbH (Hrsg.)

in Kooperation mit dem
Software Innovation Lab
der Universität Paderborn



IMPRESSUM

Herausgeber

cum ratione gGmbH

Vattmannstraße 3
33100 Paderborn

Tel: 05251 - 297 4040

Mail: info@cum-ratione.org

in Kooperation mit:

Software Innovation Lab der Universität Paderborn

Zukunftsmeile 2
33102 Paderborn

Tel: 05251 - 606820

Mail: info@sicp.de

Redaktion

Kerstin Haarmann, LL.M. MBA, cum ratione gGmbH (v. i. S. d. P.)

Dr. Simon Oberthür, Universität Paderborn

Lara Schröder, cum ratione gGmbH

Lena Wiewel, cum ratione gGmbH



cum ratione

Gesellschaft für Aufklärung und Technik gGmbH



UNIVERSITÄT
PADERBORN

SICP

www.cum-ratione.org | www.sicp.de



Maßnahmenliste für mehr Digitale Souveränität

Von Februar bis Juni 2026 hat die gemeinnützige Gesellschaft cum ratione gGmbH gemeinsam mit dem Software Innovation Lab der Universität Paderborn am SICP – Software Innovation Campus Paderborn eine **vierteilige Veranstaltungsreihe unter dem Titel „Digitale Souveränität – demokratische Antworten für ein freies Internet“** durchgeführt.

Zur Veranstaltungsreihe gehörten ein Vortrag des Medienwissenschaftlers Prof. Dr. Martin Andree, eine Podiumsdiskussion mit Vertreterinnen und Vertretern aus Politik, Medien und regionaler IT-Wirtschaft sowie ein digitales Follow-up, in dem ein auf den Erkenntnissen aus den bisherigen Veranstaltungen basierender Maßnahmenkatalog vorgestellt und diskutiert wurde. Den Abschluss der Reihe bildete ein Workshop für interessierte Privatpersonen mit dem Ziel, die eigene Kompetenz und Selbstbestimmtheit im digitalen Raum zu stärken.

Bei diesem Dokument handelt es sich um die schriftliche Ausarbeitung der im digitalen Follow-up vorgestellten Lösungsansätze. Die Maßnahmen sind dabei aufgeteilt in die folgenden fünf Hauptkategorien: **Alternativen zu Big Tech stärken, Notwendige Gesetzliche Regulierung, Sicherheit, Wirtschaft, Bildung und Gesellschaft.**

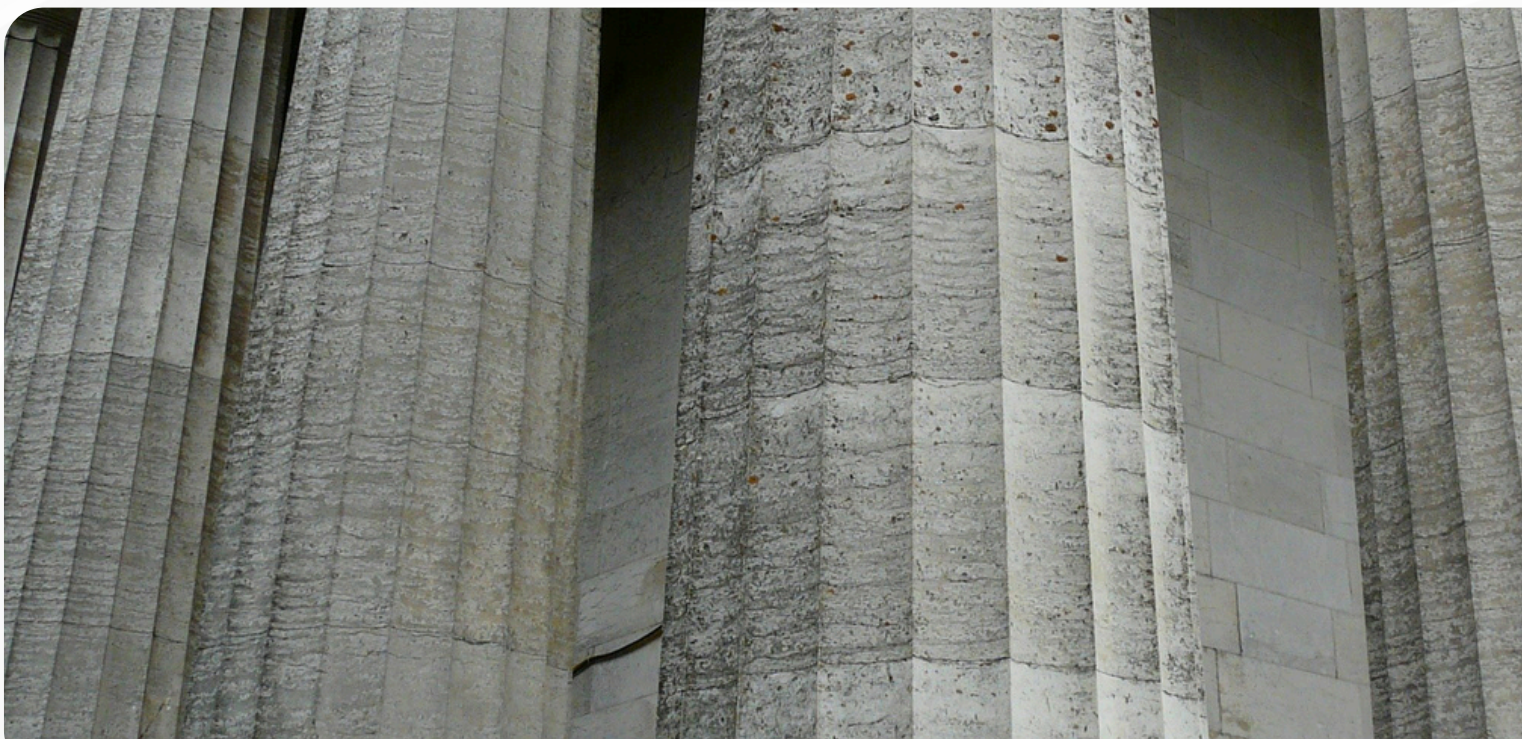
Zu jeder Kategorie werden im Papier verschiedene Maßnahmen vorgestellt, die aus Sicht der herausgebenden Organisationen zukünftig umgesetzt werden sollten. Ziel ist die übersichtliche Darstellung vielfältiger Lösungsansätze auf dem Weg zu mehr digitaler Souveränität in unserer Gesellschaft.

Für die Erarbeitung der im Paper aufgeführten Maßnahmen haben wir mehrere Quellen herangezogen. Zunächst haben wir unsere Veranstaltungsreihe und die daraus gewonnenen Erkenntnisse als Basis unseres Papiers genutzt und diese dann im nächsten Schritt mit entsprechenden Quellen belegt. Hier sind insbesondere die Publikationen von Prof. Dr. Martin Andree sowie die Empfehlungen der Initiative Save Social hervorzuheben.

Digitale Souveränität steht auf drei Säulen

1. Für Bürgerinnen und Bürger sollte eine **Absicherung der Teilhabe unter Wahrung der Entscheidungsfreiheit des Einzelnen im Umgang mit Daten** als Ziel verfolgt werden. Neben der Durchsetzung der Datenschutz-Grundverordnung sollten ergänzende infrastruktur-, medien- bzw. plattformspezifische Schutzmechanismen zu diesem Zweck eingeführt werden.
2. Im Bereich der privatwirtschaftlich agierenden Akteure in datenbasierten Märkten sollten entsprechende **Regulierungen zu Transparenz und Fairness insbesondere KMU und Newcomern den Einstieg erleichtern**.
3. Die **Verfügbarkeit und Integrität von Dateninfrastruktur** sollte **für privatwirtschaftliche Unternehmen sowie Einzelstaaten bzw. Staatenunionen** sichergestellt werden. Hierzu wurden in der Vergangenheit in der EU sowie der Bundesrepublik bereits verschiedene Rechtsakte erlassen.

Vgl. Prof. Dr. Stefan Müller: Schlüssel zur Resilienz. Drei Perspektiven aus dem Innovationsbereich Digitale Souveränität. In: Update. Das Magazin des SICP – Software Innovation Campus Paderborn, S. 48–51.



Executive Summary

Digitale Technologien spielen in unserer Gesellschaft eine immer größere Rolle. Zentrale Teile dieser Infrastruktur konzentrieren sich zurzeit allerdings auf wenige, überwiegend außereuropäische Technologieunternehmen. Damit entstehen Abhängigkeiten, die wirtschaftliche, technologische und sicherheitsrelevante Auswirkungen haben und zugleich das gesellschaftliche Zusammenleben und unsere Demokratie beeinflussen.

Digitale Souveränität bedeutet dabei nicht technologische Autarkie oder Abschottung. Sie bezeichnet die Fähigkeit von Bürgerinnen und Bürgern, Unternehmen und Staat, digitale Technologien selbstbestimmt zu nutzen, kritische Abhängigkeiten zu erkennen und zu reduzieren sowie bei Bedarf auf tragfähige Alternativen wechseln zu können.

Das Papier entwickelt dafür **konkrete Handlungsvorschläge in fünf miteinander verbundenen Bereichen:**

Alternativen zu Big Tech stärken: Offene Standards, Interoperabilität und Datenportabilität sollen Wechselmöglichkeiten schaffen und Lock-in-Effekte reduzieren. Öffentliche Investitionen und Beschaffung sollten Open Source und europäische Technologien nicht nur fördern, sondern auch deren langfristige Wartbarkeit, Produktreife und Wettbewerbsfähigkeit stärken. Öffentliche Einrichtungen sollen schrittweise auf souveräne digitale Lösungen umstellen und öffentliche Inhalte nach der +1-Regel zusätzlich über offene Standards zugänglich machen.

Gesetzliche Regulierung wirksam gestalten: Bestehende Instrumente wie DMA, DSA, DSGVO und Wettbewerbsrecht müssen konsequent angewendet und durchgesetzt werden. Zusätzlich sollen insbesondere die medienrechtliche Verantwortung marktprägender Plattformen, Haftungs- und Sorgfaltspflichten, Kartellrecht, Urheberrecht und Rechtsbehelfe weiterentwickelt werden. Regulierung soll sich dabei am tatsächlichen Einfluss und an der Marktmacht digitaler Plattformen orientieren.

Sicherheit und Resilienz stärken: Die Bundesregierung braucht eine verbindliche ressortübergreifende Strategie für digitale Souveränität. Kritische technologische Abhängigkeiten müssen systematisch erfasst und reduziert, IT-Sicherheit und Resilienz verbindlich in Infrastrukturinvestitionen integriert und starke Verschlüsselung konsequent umgesetzt werden. Dazu gehören auch professionelles Schlüsselmanagement, Krypto-Agilität und die Post-Quantum-Migration.

Wirtschaftliche Handlungsfähigkeit erhöhen: Für kritische digitale Technologien braucht es überprüfbare Souveränitätsanforderungen, tragfähige Open-Source-Ökosysteme und anbieterneutrale Transferstrukturen, die Unternehmen bei Bewertung, Erprobung und Migration unterstützen. Europäische Schlüsseltechnologien benötigen zudem langfristiges Wachstums- und Skalierungskapital sowie eine engere Verzahnung von Forschung, Transfer, öffentlicher Beschaffung und privatem Kapital.

Bildung und gesellschaftliche Selbstbestimmung sichern: Digitale Souveränität setzt sowohl Kompetenzen als auch echte Wahlmöglichkeiten voraus. Bildungseinrichtungen sollen souveräne Infrastrukturen nutzen und produktunabhängige digitale Kompetenzen vermitteln. Bürgerinnen und Bürger müssen digitale Angebote selbstbestimmt nutzen oder ablehnen können, ohne von gesellschaftlicher Teilhabe ausgeschlossen zu werden. Vereine, Organisationen und Parteien können als Multiplikatoren dazu beitragen, offene und souveräne digitale Angebote stärker zu etablieren.

Digitale Souveränität ist damit keine einzelne technologiepolitische Maßnahme, sondern eine gemeinsame Aufgabe von Politik, Wirtschaft, Wissenschaft und Gesellschaft. Ziel ist nicht Abschottung, sondern die Fähigkeit, digitale Technologien sicher und selbstbestimmt unter Wahrung eigener Handlungs- und Wahlmöglichkeiten zu nutzen und weiterzuentwickeln.

1

ALTERNATIVEN ZU BIG TECH STÄRKEN

Die Stärkung von Alternativen zu Big Tech ist ein zentraler Baustein für mehr digitale Souveränität in Deutschland und Europa. Nur wenn nachhaltige Alternativen sichtbar, zugänglich und wettbewerbsfähig sind, kann ein vielfältigeres und resilienteres digitales Ökosystem entstehen.

10

GESETZLICHE REGULIERUNGEN

Damit sich offene und souveräne Lösungen im Wettbewerb behaupten können, benötigen sie sowohl einen fairen und wirksamen rechtlichen Ordnungsrahmen als auch dessen konsequente Weiterentwicklung und Durchsetzung.

23

SICHERHEIT

Störungen, Cyberangriffe oder der Ausfall einzelner Anbieter können weitreichende Folgen für das öffentliche Leben und die wirtschaftliche Stabilität haben. Digitale Souveränität ist damit zentraler Bestandteil moderner Sicherheits- und Verteidigungspolitik.

32

WIRTSCHAFT

Digitale Technologien sind eine zentrale Grundlage wirtschaftlicher Wertschöpfung. Abhängigkeiten wirken sich bereits im normalen Wirtschaftsbetrieb aus und bedeuten in geopolitischen oder wirtschaftlichen Krisensituationen erhebliche Risiken für die wirtschaftliche Handlungsfähigkeit. Digitale Souveränität ist daher auch Wirtschafts-, Innovations- und Standortpolitik.

42

BILDUNG & GESELLSCHAFT

Digitale Souveränität ist sowohl eine Bildungs- als auch eine gesellschaftspolitische Aufgabe. Sie setzt zum einen Menschen voraus, die digitale Systeme verstehen, kritisch beurteilen und selbstbestimmt nutzen können, und zugleich müssen Staat, Wirtschaft, Bildungseinrichtungen und Technologieanbieter Rahmenbedingungen schaffen, die Teilhabe und echte Wahlmöglichkeiten ermöglichen.



ALTERNATIVEN ZU BIG TECH STÄRKEN

Die Stärkung von Alternativen zu Big Tech ist ein zentraler Baustein für mehr digitale Souveränität in Deutschland und Europa. Offene, gemeinwohlorientierte und interoperable Lösungen schaffen die Grundlage dafür, digitale Infrastrukturen unabhängiger zu gestalten, Innovation zu fördern und Abhängigkeiten von einzelnen marktbeherrschenden Plattformen zu reduzieren.

Damit solche Alternativen langfristig erfolgreich sein können, müssen sie gezielt entwickelt, eingesetzt und in ihrer Wettbewerbsfähigkeit gestärkt werden. Dies umfasst insbesondere die Förderung offener Standards, die Unterstützung europäischer Anbieter und gemeinwohlorientierter Projekte sowie die Schaffung besserer Rahmenbedingungen für den Einsatz souveräner digitaler Lösungen in Verwaltung, Wirtschaft und Gesellschaft. **Nur wenn nachhaltige Alternativen sichtbar, zugänglich und wettbewerbsfähig sind, kann ein vielfältigeres und resilienteres digitales Ökosystem entstehen.**

ALTERNATIVEN ZU BIG TECH STÄRKEN

- 1 Durchsetzung offener Standards und Interoperabilität
- 2 Faire Datennutzung statt Datenmonopole
- 3 +1-Regel: Öffentliche Inhalte zusätzlich über offene Standards bereitstellen
- 4 Strategische Investitionen in Open Source und europäische Technologien
- 5 Transformation öffentlicher Einrichtungen hin zu souveränen digitalen Lösungen

1 DURCHSETZUNG OFFENER STANDARDS UND INTER-OPERABILITÄT

Digitale Souveränität setzt voraus, dass Menschen und Organisationen ihre Kommunikations- und Informationsplattformen frei wählen können, ohne dabei Kontakte, Inhalte oder Funktionalitäten zu verlieren. Offene Standards und Interoperabilität helfen dabei, Abhängigkeiten von einzelnen Plattformen zu reduzieren. Sie schaffen faire Wettbewerbsbedingungen, ermöglichen Innovationen durch neue Marktteilnehmer und verhindern, dass einzelne Unternehmen ihre Marktmacht durch technische Abschottung dauerhaft absichern.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Regulierung von Gatekeepern:** Für Gatekeeper im Sinne des Gesetzes über digitale Märkte (Digital Markets Act, DMA) und – soweit erforderlich – weitere marktbeherrschende Plattformen müssen wirksame Anforderungen an Offenheit, Datenportabilität und Interoperabilität gelten.¹
- **Offene Standards:** Marktbeherrschende Plattformen sollten verpflichtet werden, ihre Dienste und Inhalte über dokumentierte, offene Standards zugänglich zu machen, damit Nutzende Angebote herstellerunabhängig verwenden und bei einem Angebotswechsel ihre Inhalte nicht verlieren.²
- **Umfassende Datenportabilität:** Nutzende müssen die von ihnen bereitgestellten oder durch ihre Nutzung erzeugten Daten in standardisierten, maschinenlesbaren Formaten exportieren und – soweit rechtlich und technisch möglich – direkt zu anderen Anbietern übertragen können. Bestehende Portabilitätsrechte müssen wirksam umgesetzt und technisch leicht nutzbar ausgestaltet werden.³
- **Outlink-Freiheit und Nichtdiskriminierung:** Plattformen dürfen externe Inhalte und Dienste gegenüber eigenen Angeboten weder technisch noch algorithmisch benachteiligen. Beiträge dürfen nicht allein deshalb schlechter gerankt oder in ihrer Sichtbarkeit eingeschränkt werden, weil sie auf externe Angebote verweisen.⁴
- **Interoperabilität wirksam umsetzen und erweitern:** Die bestehenden Interoperabilitätsanforderungen für Gatekeeper-Messengerdienste müssen konsequent umgesetzt werden. Nutzende sollen sicher und datenschutzkonform mit Nutzenden anderer Dienste kommunizieren können – dieses Prinzip kennen wir bereits von E-Mail, Telefon und SMS. Eine Ausweitung auf soziale Netzwerke sollte geprüft werden, sofern Datenschutz, IT-Sicherheit und gegebenenfalls bestehende Ende-zu-Ende-Verschlüsselung gewährleistet bleiben.⁵

Digitale Souveränität bedeutet Wahlfreiheit. Wahlfreiheit entsteht nur dann, wenn Nutzerinnen und Nutzer Plattformen wechseln können, ohne ihre sozialen Beziehungen, Inhalte oder digitale Identität zu verlieren.

2 FAIRE DATENNUTZUNG STATT DATENMONOPOLE

Daten sind zu einem zentralen Rohstoff der digitalen Wirtschaft geworden. Große Digitalkonzerne verfügen aufgrund ihrer enormen Nutzerbasis über Datenbestände, die ihnen erhebliche Wettbewerbsvorteile verschaffen und den Markteintritt neuer Anbieter erschweren. Ziel digitaler Souveränität darf jedoch nicht sein, möglichst viele Daten frei verfügbar zu machen, sondern ihre Nutzung so zu gestalten, dass Innovation, Wettbewerb und der Schutz der Grundrechte gleichermaßen gestärkt werden.

Die informationelle Selbstbestimmung und der Schutz personenbezogener Daten sind wesentliche Bestandteile einer souveränen digitalen Gesellschaft. Gleichzeitig benötigen Forschung, Wirtschaft und Verwaltung einen verantwortungsvollen Zugang zu Daten, um Innovationen entwickeln zu können. Dieser Zielkonflikt sollte nicht durch eine pauschale Freigabe von Daten gelöst werden, sondern durch datenschutzfreundliche und vertrauenswürdige Rahmenbedingungen.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Konsequente Datensparsamkeit:** Der Grundsatz, nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten zu erheben und zu speichern, muss technisch und organisatorisch konsequent umgesetzt werden. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen müssen zum Regelfall werden.⁶
- **Stärkung souveräner europäischer Datenräume:** Gemeinsame europäische Datenräume ermöglichen den kontrollierten Austausch von Daten zwischen Wirtschaft, Wissenschaft und öffentlicher Hand. Sie müssen auf europäischen Datenschutzstandards, offenen Schnittstellen, transparenten Governance-Regeln und der Kontrolle der Beteiligten über ihre Daten beruhen.⁷
- **Datenschutzfreundliche Forschungszugänge:** Forschung und Innovation benötigen Zugang zu hochwertigen Daten. Dieser sollte über sichere und kontrollierte Verfahren erfolgen, beispielsweise durch geschützte Forschungsumgebungen, datenschutzgerecht aufbereitete Datensätze oder wirksam anonymisierte Daten. Das Risiko einer Re-Identifizierung muss nach dem Stand der Technik bewertet, durch geeignete technische und organisatorische Maßnahmen minimiert und regelmäßig überprüft werden. Forschungseinrichtungen, Datenhalter und zuständige Zugangsstellen müssen zugleich die notwendigen Kompetenzen für Anonymisierung, Datenschutz, Informationssicherheit und eine verantwortungsvolle Datennutzung aufbauen.^{8,9}

Datenschutzwahrende Technologien ermöglichen es, Erkenntnisse aus Daten zu gewinnen, ohne sensible Informationen unnötig offenzulegen. Beim föderierten Lernen verbleiben Trainingsdaten beispielsweise in den beteiligten Organisationen oder auf lokalen Geräten; ausgetauscht werden lediglich Modellinformationen. Secure Multi-Party Computation ermöglicht mehreren Beteiligten gemeinsame Berechnungen, ohne dass sie ihre jeweiligen Ausgangsdaten gegenseitig offenlegen müssen.

Differential Privacy reduziert durch gezielte statistische Veränderungen das Risiko, einzelne Personen aus Ergebnissen herauszuerkennen.





Diese Verfahren ersetzen weder Datensparsamkeit noch rechtliche und organisatorische Schutzmaßnahmen. Ihre Wirksamkeit hängt von der konkreten Ausgestaltung, einer sicheren technischen Umsetzung und ausreichend qualifiziertem Personal ab.^{10, 11, 12}

- **Datentreuhandmodelle wettbewerblich ausgestalten:** Unabhängige Datentreuhänder können Daten im Interesse der Betroffenen verwalten und deren Nutzung transparent, nachvollziehbar und zweckgebunden steuern. Sie müssen neutral handeln und dürfen die vermittelten Daten nicht für eigene wirtschaftliche Zwecke nutzen. Offene Schnittstellen, Datenportabilität und interoperable Strukturen müssen verhindern, dass neue Abhängigkeiten oder monopolartige Vermittlungsstrukturen entstehen.¹³
- **Förderung datenschutzwahrender Technologien:** Verfahren wie föderiertes Lernen, Privacy-Preserving AI, Secure Multi-Party Computation oder Differential Privacy ermöglichen die Entwicklung leistungsfähiger KI-Systeme, ohne dass sensible personenbezogene Daten zentral zusammengeführt werden müssen.^{14, 15}
- **Verhinderung von Datenmonopolen:** Die europäische Wettbewerbs- und Datenpolitik sollte Datenmonopole durch wirksame Portabilitäts-, Interoperabilitäts- und Zugangsrechte sowie eine konsequente Durchsetzung des Wettbewerbsrechts begrenzen. Personenbezogene Daten dürfen dabei nicht gegen den Willen der Betroffenen geöffnet oder weitergegeben werden.¹⁶

Digitale Souveränität bedeutet, dass Menschen, Organisationen und Staaten bestimmen können, wer ihre Daten zu welchem Zweck nutzt. **Datenschutz und Datensouveränität sind dabei kein Innovationshemmnis, sondern können zu einem europäischen Wettbewerbsvorteil werden:** Datenschutzwahrende Technologien und vertrauenswürdige Datenräume schaffen die Grundlage für Innovation, gesellschaftliches Vertrauen und fairen Wettbewerb.

3 +1-REGEL: ÖFFENTLICHE INHALTE ZUSÄTZLICH ÜBER OFFENE STANDARDS BEREITSTELLEN

Die öffentliche Hand trägt eine besondere Verantwortung für eine offene, zugängliche und unabhängige digitale Informationsinfrastruktur. Werden öffentliche Informationen ausschließlich über Plattformen einzelner Digitalkonzerne verbreitet, verstärkt dies deren Marktmacht und zwingt Bürgerinnen und Bürger faktisch dazu, diese Plattformen zu nutzen. Gleichzeitig bleiben offene und föderierte Alternativen oft unsichtbar und können die für ihren Erfolg notwendigen Netzwerkeffekte kaum erreichen.

Die +1-Regel verfolgt deshalb einen pragmatischen Ansatz: Staatliche Einrichtungen sollen bestehende Kommunikationskanäle nicht zwingend aufgeben, sondern öffentliche Informationen grundsätzlich zusätzlich über Plattformen und Dienste bereitstellen, die auf offenen und anerkannten Standards sowie Protokollen basieren.

Wir schlagen deshalb folgende Maßnahmen vor: ¹⁷

- **+1-Regel:** Alle mit öffentlichen Mitteln finanzierten Inhalte müssen mindestens zusätzlich auf Plattformen oder Diensten veröffentlicht werden, die auf offenen und anerkannten Standards sowie Protokollen basieren.
- **Öffentliche Einrichtungen:** Die +1-Regel soll für Bund, Länder, Kommunen, Behörden, Hochschulen, Forschungseinrichtungen, Bibliotheken sowie den öffentlich-rechtlichen Rundfunk gelten.
- **Öffentliche Mediatheken:** Öffentliche Informations- und Medienangebote, beispielsweise Mediatheken oder Presseportale, sollen ihre Inhalte über Protokolle zugänglich machen und so die Weiterverbreitung durch alternative Dienste ermöglichen.
- **Automatisierte Mehrfachveröffentlichung:** Inhalte sollten möglichst medienneutral erstellt und über geeignete Schnittstellen automatisiert für unterschiedliche Kanäle bereitgestellt werden. Plattformspezifische Anpassungen und eine redaktionelle Qualitätssicherung bleiben dabei erforderlich; der zusätzliche Aufwand kann durch gemeinsame technische Werkzeuge deutlich reduziert werden.¹⁸
- **Vorbildfunktion des Staates:** Die öffentliche Hand soll ihre Reichweiten-, Nachfrage- und Gestaltungsmacht nutzen, um offene Standards, Interoperabilität und digitale Souveränität zu fördern und dadurch Innovation sowie Wettbewerb zu stärken.

Die +1-Regel schafft keine Einschränkung bestehender Kommunikationswege, sondern erweitert sie. Sie stärkt offene digitale Infrastrukturen, ohne Bürgerinnen und Bürger oder öffentliche Einrichtungen zum Verzicht auf bestehende Plattformen zu zwingen.

4 STRATEGISCHE INVESTITIONEN IN OPEN SOURCE UND EUROPÄISCHE TECHNOLOGIEN

Der Markt allein wird digitale Souveränität in Europa nicht herstellen. Große Digitalkonzerne verfügen über erhebliche Wettbewerbsvorteile durch Kapital, Daten, Netzwerkeffekte und bestehende Marktpositionen. Deutschland und Europa benötigen deshalb eine aktive Innovations- und Industriepolitik, die gezielt offene Technologien und souveräne europäische Lösungen stärkt.

Investitionen in Open Source und europäische Technologien sind dabei kein Selbstzweck. Sie schaffen Innovationen, stärken die europäische Wertschöpfung, fördern den Wettbewerb und reduzieren langfristig strategische Abhängigkeiten von einzelnen Anbietern. Die öffentliche Hand sollte ihre erhebliche Beschaffungs- und Investitionskraft deshalb gezielt nutzen, um den Aufbau eines leistungsfähigen europäischen digitalen Ökosystems – eines European Digital Stack – voranzutreiben.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Digitale Souveränität als strategisches Vergabekriterium:** In öffentlichen Ausschreibungen sollten neben Preis und Lebenszykluskosten insbesondere Offenheit, Interoperabilität, IT-Sicherheit, Wartbarkeit, Exit-Strategien sowie die Vermeidung von *Vendor-Lock-in* berücksichtigt werden.¹⁹



Vendor Lock-in bezeichnet die Abhängigkeit von einem bestimmten Technologieanbieter. Ein Wechsel zu einer anderen Lösung ist oft mit hohen Kosten, großem Aufwand oder technischen Hürden verbunden.

Die Ursachen können beispielsweise proprietäre Dateiformate, Schnittstellen oder Datenstrukturen sein, die einen Wechsel erschweren. Die Abhängigkeit davon kann zusätzlich dazu führen, dass Anbieterwechsel ausbleiben – selbst wenn bessere Alternativen verfügbar wären.

Dadurch werden Wahlfreiheit und digitale Souveränität eingeschränkt.

- **Bevorzugte Berücksichtigung offener und europäischer Lösungen:** Sind Angebote unter Berücksichtigung von Funktionalität, Sicherheit, Lebenszykluskosten, Wartbarkeit und Support gleichwertig, sollten Open-Source-Software und souveräne europäische Alternativen bevorzugt berücksichtigt werden.²⁰
- **Langfristige Förderung von Open Source:** Open-Source-Projekte benötigen eine nachhaltige Finanzierung über den gesamten Lebenszyklus. Förderprogramme sollten deshalb nicht nur die Entwicklung neuer Software, sondern auch Wartung, Sicherheitsupdates, Dokumentation, Community-Arbeit und langfristigen Betrieb unterstützen.²¹

- **Investitionen in den European Digital Stack:** EU, Bund und Länder sollten gezielt in den Aufbau einer leistungsfähigen europäischen digitalen Infrastruktur investieren. Dazu gehören beispielsweise Cloud- und Rechenzentrumsdienste, digitale Identitäten, Datenräume, Kommunikationsplattformen, KI-Infrastrukturen sowie weitere Schlüsseltechnologien auf Basis offener Standards.²²
- **Förderung von Innovation und Wettbewerb:** Öffentliche Investitionen sollten insbesondere KMU, Start-ups und Technologieanbietern mit substanzieller europäischer Wertschöpfung, Entwicklung und Kontrolle beim Markteintritt und der Skalierung unterstützen.²³

Digitale Souveränität entsteht nicht allein durch Regulierung. Sie erfordert auch den gezielten **Aufbau eigener technologischer Kompetenzen und leistungsfähiger europäischer Alternativen**. Die öffentliche Hand sollte ihre Investitions- und Beschaffungskraft deshalb strategisch nutzen, um langfristig einen offenen, sicheren und wettbewerbsfähigen European Digital Stack zu aufzubauen.

5 TRANSFORMATION ÖFFENTLICHER EINRICHTUNGEN HIN ZU SOUVERÄNEN DIGITALEN LÖSUNGEN

Die öffentliche Verwaltung muss ihre digitale Handlungsfähigkeit langfristig sichern. In vielen Bereichen bestehen erhebliche Abhängigkeiten von einzelnen Softwareanbietern – beispielsweise bei Bürosoftware, Cloud-Diensten, Kollaborationsplattformen oder Fachverfahren. Diese Abhängigkeiten führen zu hohen Wechselkosten, erschweren den Wettbewerb und bergen sicherheits- sowie geopolitische Risiken. Ziel muss daher eine schrittweise Transformation hin zu einer souveränen, offenen und langfristig kontrollierbaren digitalen Infrastruktur sein.

Open-Source-Software und souveräne europäische Lösungen sind dabei kein Selbstzweck, sondern ein wichtiger Baustein, um Transparenz, Interoperabilität und langfristige Unabhängigkeit sicherzustellen, sowie gleichzeitig Wettbewerb und Innovationen zu fördern.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Transformationsstrategie:** Bund, Länder und Kommunen sollen eine langfristige Strategie zur schrittweisen Umstellung ihrer digitalen Infrastruktur auf souveräne Lösungen entwickeln. Die Migration sollte planbar, risikobasiert und wirtschaftlich erfolgen.²⁴
- **Bevorzugung souveräner Lösungen:** Bei Neuanschaffungen und Modernisierungen müssen offene Standards, Interoperabilität, Datenportabilität und Exit-Strategien von Beginn an berücksichtigt werden, um neue Abhängigkeiten zu vermeiden. Wo funktional und wirtschaftlich vertretbar, sollten Open-Source-Software und souveräne europäische Alternativen bevorzugt eingesetzt werden.²⁵
- **Kompetenzaufbau und Change Management:** Die öffentliche Verwaltung muss eigenes technisches Know-how aufbauen – zentrale Kompetenzen für Betrieb, Wartung und Weiterentwicklung dürfen nicht ausschließlich bei externen Dienstleistern liegen. Umstellungen auf neue Lösungen müssen dabei durch ein professionelles Change Management, beispielsweise Schulungsangebote und Migrationshilfen, begleitet werden.²⁶
- **Offene Dokumenten- und Datenaustauschformate:** Öffentliche Einrichtungen sollten konsequent auf offene Formate setzen, um den langfristigen Zugriff auf Informationen sicherzustellen und den Wechsel zwischen verschiedenen Softwarelösungen zu erleichtern.²⁷

Digitale Souveränität entsteht nicht allein durch die Auswahl einer bestimmten Software. Entscheidend ist, dass die öffentliche Verwaltung ihre digitale Infrastruktur langfristig selbst gestalten, sicher betreiben und unabhängig weiterentwickeln kann. Diese schrittweise Transformation stärkt nicht nur die Resilienz des Staates, sondern setzt zugleich wichtige **Impulse für Innovation, Wettbewerb und europäische Eigenständigkeit.**

A bronze statue of a blindfolded figure, likely representing justice, holding a set of scales. The statue is positioned on the right side of the frame, with its head turned slightly to the left. The background is a warm, orange-brown gradient. The text is overlaid on the lower left portion of the image.

NOTWENDIGE GESETZLICHE REGULIERUNGEN

Die Stärkung von Alternativen ist von großer Bedeutung, damit in Deutschland und Europa verstärkt souveräne technische Lösungen entwickelt und wettbewerbsfähig gemacht werden. Alternativen allein reichen jedoch nicht aus. **Damit sich offene und souveräne Lösungen im Wettbewerb behaupten können**, benötigen sie sowohl einen fairen und wirksamen rechtlichen Ordnungsrahmen als auch dessen konsequente Weiterentwicklung und Durchsetzung.

Ziel ist es, fairen Wettbewerb zu ermöglichen, Innovationskraft zu stärken und die Konzentration von Marktmacht einzelner marktbeherrschender Plattformen zu begrenzen. Neben der konsequenten Durchsetzung bereits existierender Gesetze sollte der Rechtsrahmen für digitale Plattformen weiterentwickelt und insbesondere bei marktprägenden und meinungsrelevanten Plattformen an deren wirtschaftlichen, gesellschaftlichen und demokratischen Einfluss angepasst werden. Dazu gehört beispielsweise die Einordnung der sozialen Medien unter den bestehenden medienrechtlichen Ordnungsrahmen, um ungerechtfertigte Privilegien marktbeherrschender Plattformen abzubauen.²⁸

NOTWENDIGE GESETZLICHE REGULIERUNGEN

- 1 Bestehende Gesetze konsequent durchsetzen
- 2 Medienrechtliche Verantwortung meinungsrelevanter Plattformen weiterentwickeln
- 3 Haftungs- und Sorgfaltspflichten an den tatsächlichen Einfluss digitaler Plattformen anpassen
- 4 Einführung einer europäischen Digitalsteuer – Besteuerung am Ort der wirtschaftlichen Wertschöpfung
- 5 Modernisierung des Kartellrechts für digitale Plattformmärkte
- 6 Urheberrecht im Zeitalter generativer KI durchsetzen und weiterentwickeln
- 7 Wirksame und unabhängige Rechtsbehelfe gegen Plattformentscheidungen

“

Vieles hängt von Rechtsregeln ab. Diese Regeln so auszugestalten, dass das Netz wieder befreit wird, ist möglich.²⁹

”

Andree & Pfeiffer

1

BESTEHENDE GESETZE KONSEQUENT DURCHSETZEN

Europa verfügt bereits über einen modernen Rechtsrahmen für digitale Märkte und Plattformen. Mit dem Digital Markets Act (DMA), dem Digital Services Act (DSA) sowie weiteren europäischen Regelwerken wurden wichtige Grundlagen geschaffen, um fairen Wettbewerb zu fördern, Grundrechte zu schützen und die Marktmacht großer Plattformen zu begrenzen. Digitale Souveränität entsteht jedoch nicht allein durch neue Gesetze, sondern vor allem durch konsequente und wirksame Durchsetzung.

Derzeit besteht häufig kein Regelungs-, sondern ein Vollzugsdefizit. Langwierige Verfahren, begrenzte personelle und technische Ressourcen sowie die internationale Struktur großer Digitalkonzerne erschweren eine wirksame Rechtsdurchsetzung. Dadurch entstehen Wettbewerbsnachteile für Unternehmen, die sich an europäische Regeln halten, während Verstöße oftmals nur verzögert oder unzureichend sanktioniert werden.³⁰

Der **Digital Markets Act (DMA)**, der am 1. November 2022 in Kraft getreten ist, verfolgt das Ziel, die Märkte im digitalen Sektor fairer und wettbewerbsfähiger zu gestalten und damit die Macht der großen Digitalkonzerne zu regulieren. Dazu beinhaltet der DMA verschiedene klar definierte und objektive Kriterien, im Rahmen derer sogenannte Gatekeeper identifiziert werden können. Dabei handelt es sich um große digitale Plattformen, wie beispielsweise Online-Suchmaschinen, App-Stores und Messenger-Dienste. Gatekeeper müssen die im EU-Gesetz aufgelisteten Verpflichtungen und Verbote beachten, wie zum Beispiel die Gewährleistung von Interoperabilität in bestimmten Situationen oder das Verbot, eigene Produkte und Dienstleistungen im Ranking auf der Plattform besser darzustellen.³¹

Der **Digital Services Act (DSA)** gilt seit Februar 2024 in der Europäischen Union und soll einen sichereren digitalen Raum schaffen, in dem die Grundrechte aller Nutzerinnen und Nutzer digitaler Dienste im EU-Binnenmarkt geschützt sind. Die Plattformen sollen dafür sorgen, dass illegale Inhalte entfernt werden, und sie müssen das Risiko minimieren, dass illegale Inhalte auf die Plattformen gelangen. Zu den Maßnahmen gehören beispielsweise gezielte Schutzmaßnahmen für Betroffene von Online-Belästigungen, die Einführung kostenloser Beschwerde-mechanismen oder das Verbot bestimmter Arten von gezielter Werbung. Für die besonders großen Online-Plattformen (VLOPs = *Very Large Online Platforms*), wie beispielsweise X oder Meta, und die sehr großen Suchmaschinen sind besondere Vorschriften vorgesehen.^{32, 33}

Wir schlagen deshalb folgende Maßnahmen vor:

- **Konsequente Anwendung bestehender Gesetze:** Der Digital Markets Act (DMA), der Digital Services Act (DSA), die Datenschutz-Grundverordnung (DSGVO) sowie weitere europäische Regelwerke müssen konsequent angewendet und durchgesetzt werden.
- **Stärkung der Aufsichtsbehörden:** Die zuständigen europäischen und nationalen Behörden müssen personell, technisch und finanziell so ausgestattet werden, dass sie Verstöße wirksam verfolgen und komplexe digitale Märkte beaufsichtigen können.^{34, 35}
- **Wirksame Sanktionen:** Verstöße gegen europäische Regelungen müssen zeitnah und spürbar sanktioniert werden, damit Rechtsverstöße keinen wirtschaftlichen Vorteil darstellen.³⁶
- **Europäische Koordination:** Die Zusammenarbeit der zuständigen Behörden innerhalb Europas sollte weiter gestärkt werden, um eine einheitliche und wirksame Durchsetzung gegenüber international agierenden Plattformen sicherzustellen.
- **Regelmäßige Evaluation:** Die Wirksamkeit bestehender Regelungen sollte regelmäßig überprüft und dort weiterentwickelt werden, wo neue technologische Entwicklungen oder Geschäftsmodelle dies erforderlich machen.

Ein souveräner Staat zeichnet sich nicht nur dadurch aus, dass er Regeln setzen kann, sondern auch dadurch, dass er diese gegenüber allen Marktteilnehmern wirksam durchsetzt. **Die konsequente Anwendung bestehender Gesetze schützt fairen Wettbewerb, stärkt das Vertrauen in den Rechtsstaat und ist eine wesentliche Voraussetzung digitaler Souveränität.** Voraussetzung dafür ist, dass klare Ziele definiert werden und Gesetzesregelungen sich widerspruchsfrei und wirksam um- und durchsetzen lassen.

2 MEDIENRECHTLICHE VERANTWORTUNG MEINUNGS-RELEVANTER PLATTFORMEN WEITERENTWICKELN

Digitale Plattformen haben sich zu den wichtigsten Orten der öffentlichen Meinungsbildung entwickelt. Millionen Menschen informieren sich heute überwiegend über soziale Netzwerke und Videoplattformen. Anders als klassische technische Infrastrukturen beeinflussen diese Plattformen durch algorithmische Empfehlungen und Rankingmechanismen, welche Inhalte Reichweite erzielen. Damit prägen sie den öffentlichen Diskurs und übernehmen eine Verantwortung, die weit über die eines rein technischen Vermittlers hinausgeht.

Aufbauend auf der im DSA und bestehenden medienrechtlichen Regelungen bereits begründeten Verantwortung für digitale Plattformen plädieren wir für eine stärkere Sicherung der Meinungs- und Anbietervielfalt sowie die Kontrolle algorithmischer Reichweitenentscheidungen. Während klassische Medien weitreichenden medienrechtlichen Anforderungen unterliegen, können sich marktbeherrschende Plattformen häufig auf ihre Rolle als technische Vermittler berufen – obwohl sie die öffentliche Kommunikation aktiv beeinflussen. Dies verschafft ihnen erhebliche Wettbewerbsvorteile. Gleichzeitig erzielen große Plattformen hohe Umsätze durch Werbung und andere Formen der Monetarisierung, die auf den von Dritten erstellten Inhalten basieren. Sie profitieren damit wirtschaftlich von der öffentlichen Kommunikation, ohne in vergleichbarer Weise Verantwortung für deren Gestaltung zu übernehmen.^{37, 38}

Wir schlagen deshalb folgende Maßnahmen vor:

- **Medienrechtliche Einordnung:** Plattformen, die maßgeblich zur öffentlichen Meinungsbildung beitragen, sollen den wesentlichen Anforderungen und Grundprinzipien des Medienrechts unterliegen. Hierzu gehören insbesondere: Staatsferne, Sicherung der Medien- und Anbietervielfalt, Transparenz, diskriminierungsfreie Behandlung von Inhalten, wirksame Beschwerde- und Kontrollmechanismen sowie die Förderung hochwertiger journalistischer und redaktioneller Inhalte.³⁹
- **Verantwortung für algorithmische Entscheidungen:** Wer durch Algorithmen über Sichtbarkeit, Reichweite und Monetarisierung öffentlicher Inhalte entscheidet, muss hierfür auch eine entsprechende rechtliche Verantwortung übernehmen. Die Kriterien für algorithmische Empfehlungen und Reichweitenentscheidungen müssen nachvollziehbar und überprüfbar ausgestaltet werden.⁴⁰
- **Weiterentwicklung des Medienrechts:** Der Medienstaatsvertrag und weitere medienrechtliche Regelungen sollten so weiterentwickelt werden, dass sie der Rolle großer digitaler Plattformen bei der öffentlichen Meinungsbildung angemessen Rechnung tragen.

Wer den öffentlichen Kommunikationsraum maßgeblich gestaltet und wirtschaftlich von ihm profitiert, trägt auch Verantwortung für dessen faire und transparente Ausgestaltung. Das muss für digitale Plattformen genauso gelten wie für andere Akteure mit derartigem Einfluss.⁴¹

3 HAFTUNGS- UND SORGFALTPFLICHTEN AN DEN TATSÄCHLICHEN EINFLUSS DIGITALER PLATTFORMEN ANPASSEN

Das bestehende Haftungsprivileg digitaler Plattformen stammt aus einer Zeit, in der diese vor allem als neutrale technische Vermittler fungierten. Heute übernehmen sie als marktprägende Plattformen jedoch eine deutlich aktivere Rolle: Sie entscheiden mithilfe von Algorithmen über Sichtbarkeit von Inhalten, beeinflussen öffentliche Meinungsbildung und erzielen erhebliche Werbeeinnahmen durch die Monetarisierung dieser Inhalte. Dabei können sie in Einzelfällen sogar wirtschaftlich von der Verbreitung strafbarer oder rechtswidriger Inhalte profitieren. Schätzungen zufolge soll *Meta* allein im Jahr 2024 Milliardenumsätze durch Werbeanzeigen im Umfeld von Betrugsmaschen (*Scams*) und anderen rechtswidrigen Inhalten erzielt haben.⁴²

Wer den öffentlichen Kommunikationsraum aktiv gestaltet und wirtschaftlich von den dort verbreiteten Inhalten profitiert, sollte hierfür auch eine angemessene Verantwortung übernehmen. Eine Privilegierung gegenüber klassischen Medienunternehmen ist unter diesen Voraussetzungen nicht mehr gerechtfertigt.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Haftungsregeln weiterentwickeln:** Sowohl auf europäischer als auch medienstaatsvertraglicher Ebene muss geprüft werden, wie die bestehenden Haftungsregelungen (z. B. DSA) der aktiven Rolle marktprägender Plattformen bei algorithmischer Auswahl, Empfehlung und Monetarisieren hinreichend angepasst werden können. Dabei ist klar zwischen rein technischen Vermittlungsleistungen, dem Umgang mit rechtswidrigen Nutzerinhalten und eigenen oder aktiv vermarkteten Inhalten der Plattform zu unterscheiden. Die marktprägenden Plattformen tragen die Beweislast für ihren Einfluss auf den jeweiligen Sachverhalt.⁴³
- **Verantwortung entsprechend des Einflusses:** Der Umfang der Verantwortung sollte sich danach richten, welchen Einfluss eine Plattform auf die Verbreitung und Sichtbarkeit von Inhalten ausübt. Wer aktiv Reichweiten steuert und Inhalte empfiehlt, übernimmt mehr Verantwortung als ein rein technischer Hosting-Anbieter.⁴⁴
- **Monetarisierung und Verantwortung verknüpfen:** Plattformen, die erhebliche Umsätze durch Werbung oder andere Formen der Monetarisierung von Nutzerinhalten erzielen, sollten auch eine entsprechende Verantwortung für diese Inhalte tragen.⁴⁵
- **Schutz kleiner und nicht-kommerzieller Plattformen:** Nicht-kommerzielle Plattformen, offene Communities und föderierte Netzwerke dürfen durch eine Weiterentwicklung des Haftungsrechts nicht unverhältnismäßig belastet werden. Regulierung sollte sich insbesondere auf marktbeherrschende und kommerziell agierende Plattformen konzentrieren.⁴⁶

Das Haftungsrecht sollte die tatsächliche Rolle digitaler Plattformen widerspiegeln. Wer Inhalte lediglich bereitstellt, ist anders zu behandeln als Plattformen, die öffentliche Kommunikation aktiv gestalten und wirtschaftlich von ihr profitieren. Verantwortung sollte dem tatsächlichen Einfluss auf den öffentlichen Diskurs entsprechen.

4 EINFÜHRUNG EINER EUROPÄISCHEN DIGITALSTEUER

Digitale Plattformen und Technologiekonzerne erzielen erhebliche Umsätze in Europa, doch häufig werden Gewinne in Länder mit niedrigeren Unternehmenssteuern verlagert. Dadurch entstehen Wettbewerbsnachteile für europäische Unternehmen, die ihre Wertschöpfung überwiegend vor Ort erbringen und entsprechend besteuert werden.

Digitale Souveränität setzt voraus, dass Unternehmen, die von europäischen Märkten und der öffentlichen Infrastruktur profitieren, sich auch angemessen an deren Finanzierung beteiligen. Eine Besteuerung digitaler Wertschöpfung wird auf europäischer Ebene seit Jahren diskutiert. Sowohl das Europäische Parlament als auch die Europäische Kommission haben dazu Vorschläge vorgelegt, während einzelne Mitgliedstaaten wie Frankreich, Italien und Österreich bereits nationale Digitalsteuern eingeführt und damit gezeigt haben, dass entsprechende Modelle grundsätzlich umsetzbar sind.⁴⁷

Wir schlagen deshalb folgende Maßnahmen vor:

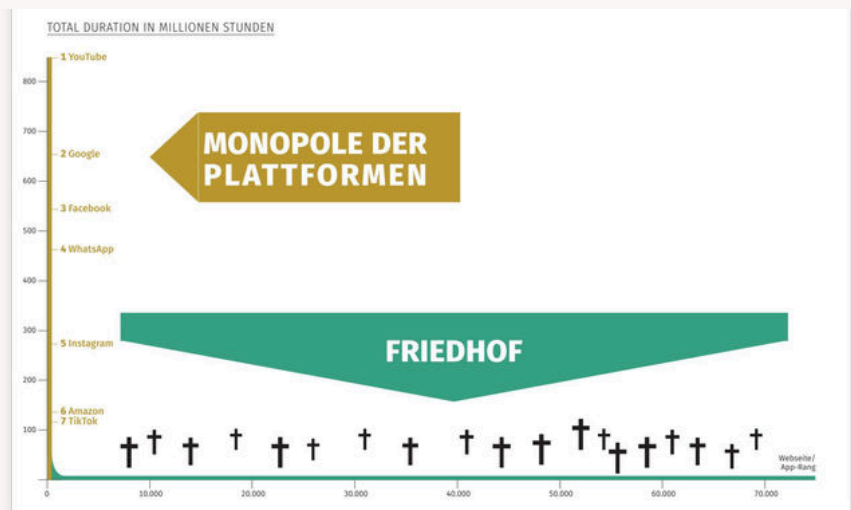
- **Einführung einer europäischen Digitalsteuer:** Eine einheitliche europäische Digitalsteuer stellt sicher, dass große Digitalkonzerne dort angemessen zur Finanzierung beitragen, wo ihre Umsätze und wirtschaftliche Wertschöpfung entstehen.⁴⁸
- **Gezielte Ausgestaltung der Digitalsteuer:** Die Digitalsteuer sollte sich auf besonders profitable digitale Geschäftsmodelle und -umsätze großer Digitalkonzerne konzentrieren, etwa Online-Werbung und digitale Vermittlungsplattformen, und digitale Grundversorgung möglichst von zusätzlichen Belastungen ausnehmen.⁴⁹
- **Investitionen in digitale Souveränität:** Zusätzliche Einnahmen aus dieser fairen Besteuerung sollten gezielt in den Aufbau digitaler Souveränität investiert werden – insbesondere in offene digitale Infrastrukturen, Cybersicherheit, Forschung, Bildung und europäische Schlüsseltechnologien.⁵⁰

Digitale Souveränität bedeutet auch fiskalische Souveränität. Unternehmen, die in Europa wirtschaftlich erfolgreich sind und von den Rahmenbedingungen des europäischen Binnenmarktes profitieren, sollten sich auch angemessen an dessen Finanzierung beteiligen. **Faire Besteuerung schafft gleiche Wettbewerbsbedingungen und stärkt die Handlungsfähigkeit Europas.** Mögliche handelspolitische Gegenmaßnahmen müssen dabei strategisch berücksichtigt werden.

5 MODERNISIERUNG DES KARTELLRECHTS FÜR DIGITALE PLATTFORMMÄRKTE

Digitale Märkte unterscheiden sich grundlegend von klassischen Märkten. Netzwerkeffekte, Datenkonzentration, Lock-in-Effekte und die Kontrolle ganzer digitaler Ökosysteme führen dazu, dass einzelne Plattformen innerhalb kurzer Zeit marktbeherrschende Stellungen erreichen können. Insbesondere Plattformen mit erheblicher Bedeutung für die öffentliche Meinungsbildung verfügen dadurch über einen außergewöhnlich großen wirtschaftlichen und gesellschaftlichen Einfluss. Dies gefährdet nicht nur den freien Wettbewerb, sondern auch die Medienvielfalt und damit eine wesentliche Grundlage demokratischer Gesellschaften.⁵¹

Das deutsche Kartellrecht wurde bereits an digitale Märkte angepasst und wird durch die Verhaltenspflichten des DMA ergänzt. Neben klassischen Marktanteilen müssen allerdings künftig auch Datenmacht, Kontrolle über digitale Infrastrukturen sowie der Einfluss auf die öffentliche Meinungsbildung stärker berücksichtigt werden. Ziel ist es nicht, erfolgreiche Unternehmen zu bestrafen, sondern faire Wettbewerbsbedingungen zu schaffen und dauerhafte Monopolstrukturen zu verhindern.



Grafik aus: Prof. Dr. Martin Andree: „Vermessung der digitalen Welt“, Campus Verlag, 2026.

Wir schlagen deshalb folgende Maßnahmen vor:⁵²

- **Marktanteilsobergrenze:** Für Plattformen mit erheblicher Bedeutung für die öffentliche Meinungsbildung sollte – analog zum Medienstaatsvertrag – eine Obergrenze von 30 % des Rezeptionsanteils innerhalb einer demokratierelevanten Kategorie gelten. Die Ermittlung des Anteils muss durch eine unabhängige Behörde erfolgen.
- **Strukturelle Entflechtung:** Plattformen mit erheblicher Bedeutung für die öffentliche Meinungsbildung sollten ihre technische Infrastruktur organisatorisch von Diensten zur Inhaltsauswahl, Empfehlung und Monetarisierung trennen. Wer die Infrastruktur bereitstellt, sollte nicht gleichzeitig über Reichweite, Sichtbarkeit und wirtschaftlichen Erfolg von Inhalten entscheiden.



Beispiel: Eine Videoplattform könnte künftig aus einer neutralen Infrastruktur für Speicherung, Suche und Videowiedergabe bestehen. Unterschiedliche Anbieter konkurrieren auf dieser Infrastruktur mit eigenen Empfehlungsalgorithmen, Kanälen und Geschäftsmodellen. So würde Wettbewerb nicht mehr um die Kontrolle der Infrastruktur, sondern um die Qualität der Inhalte und Dienste stattfinden.⁵³

- **Offene Infrastruktur:** Die technische Infrastruktur demokratierelevanter Plattformen sollte auf offenen Standards beruhen und interoperabel ausgestaltet sein. Dadurch können verschiedene Anbieter von Kommunikations- und Inhaltsdiensten auf derselben Infrastruktur im Wettbewerb miteinander stehen, während Nutzerinnen und Nutzer plattformübergreifend kommunizieren und Inhalte austauschen können.⁵⁴
- **Digitale Marktmacht wirksam kontrollieren:** Das Kartellrecht sollte bestehende Instrumente konsequent anwenden und nachgewiesene Schutzlücken schließen. Neben Marktanteilen müssen insbesondere Netzwerkeffekte, Datenmacht, Lock-in-Effekte sowie die Kontrolle über digitale Ökosysteme in kartellrechtliche Entscheidungen einfließen.⁵⁵
- **Überprüfung strategischer Übernahmen:** Die Übernahme innovativer Unternehmen durch marktbeherrschende Plattformen sollte strenger geprüft werden, um sogenannte *Killer Acquisitions* zu verhindern und den langfristigen Wettbewerb zu sichern.⁵⁶
- **Bundeseinheitliche Medienaufsicht:** Für marktprägende digitale Plattformen sollte die medienrechtliche Aufsicht bundeseinheitlich organisiert werden. Die bisherige Zersplitterung der Zuständigkeiten wird der bundesweiten und grenzüberschreitenden Bedeutung digitaler Plattformmärkte nicht mehr gerecht.
- **Stärkung der Wettbewerbsaufsicht:** Die kartell- und wettbewerbsrechtliche Aufsicht über digitale Plattformmärkte sollte – soweit keine Zuständigkeit der Europäischen Kommission besteht – beim Bundeskartellamt gebündelt und personell sowie technisch weiter gestärkt werden.⁵⁷
- **Ausreichende Ressourcen:** Die zuständigen Aufsichtsbehörden müssen mit den notwendigen personellen, technischen und finanziellen Ressourcen ausgestattet werden, um hochkomplexe digitale Plattformmärkte wirksam beaufsichtigen und regulatorische Entscheidungen zeitnah treffen zu können.

Killer Acquisitions bezeichnet Übernahmen, bei denen ein marktmächtiges Unternehmen ein innovatives Start-up kauft, um dessen Technologie, Produkte oder Wachstum zu kontrollieren und mögliche zukünftige Konkurrenz zu verhindern. Dadurch können Innovationen ausgebremst und der Wettbewerb geschwächt werden.

Wettbewerb entsteht in digitalen Märkten nicht von selbst. Wo wenige Plattformen gleichzeitig Infrastruktur, Reichweite, Algorithmen und Monetarisierung kontrollieren, entstehen strukturelle Machtkonzentrationen. **Ein modernes Kartellrecht muss deshalb sicherstellen, dass digitale Märkte offen, wettbewerbsfähig und demokratisch bleiben.**

6 URHEBERRECHT IM ZEITALTER GENERATIVER KI DURCHSETZEN UND WEITERENTWICKELN

Kreative, journalistische und wissenschaftliche Inhalte bilden eine wesentliche Grundlage für die Entwicklung und den Betrieb generativer KI-Systeme. Die wirtschaftliche Wertschöpfung darf dabei nicht einseitig bei den Anbietern dieser Systeme verbleiben. Urheberinnen und Urheber sowie andere Rechteinhaberinnen und -inhaber müssen nachvollziehen und mitbestimmen können, wie ihre geschützten Inhalte verwendet werden, und angemessen an ihrer kommerziellen Nutzung beteiligt werden.

Das geltende Urheberrecht enthält bereits Regelungen für die automatisierte Analyse von Texten und Daten. In der Praxis ist es für Rechteinhaberinnen und -inhaber jedoch häufig schwierig, festzustellen, ob ihre Werke für das Training von KI-Modellen genutzt wurden, wirksam einen Rechtevorbehalt zu erklären oder bestehende Ansprüche gegenüber international agierenden Unternehmen durchzusetzen. Das Urheberrecht muss deshalb konsequent angewendet und dort weiterentwickelt werden. Ein Beispiel hierfür sind die KI-Zusammenfassungen von Nachrichten oder Suchanfragen, die dazu führen, dass die Nutzenden gar nicht mehr auf die Links der eigentlichen Inhalteanbieter klicken. Dadurch gehen diesen Aufmerksamkeit und Werbeeinnahmen verloren.⁵⁸

Wir schlagen deshalb folgende Maßnahmen vor:

- **Durchsetzung bestehender Rechte:** Anbieter von KI-Systemen müssen geltende Urheber- und Nutzungsrechte sowie wirksam erklärte Rechtevorbehalte konsequent beachten. Bestehende Vorgaben dürfen nicht dadurch wirkungslos werden, dass Rechteinhaberinnen und -inhaber ihre Einhaltung praktisch kaum überprüfen oder durchsetzen können. Sie benötigen niedrigschwellige Beschwerde-, Auskunfts- und Durchsetzungsmöglichkeiten.⁵⁹
- **Faire Lizenz- und Vergütungsmodelle:** Für die kommerzielle Nutzung geschützter Inhalte müssen praktikable und faire Lizenzmodelle geschaffen werden. Neben individuellen Vereinbarungen sollten auch standardisierte und kollektive Modelle geprüft werden, damit nicht nur große Medienunternehmen, sondern auch einzelne Kreative und Kleinunternehmen angemessen an der Wertschöpfung beteiligt werden.⁶⁰
- **Transparenz verwendeter Inhalte:** Die Transparenzpflichten des AI Acts zu den für das Training verwendeten Inhalten müssen konsequent umgesetzt und auf ihre Wirksamkeit für die Rechtsdurchsetzung überprüft werden. Rechteinhaber müssen Rechtevorbehalte standardisiert und maschinenlesbar erklären können. Anbieter von KI-Modellen müssen solche Vorbehalte technisch zuverlässig erkennen und respektieren.⁶¹
- **Schutz journalistischer Wertschöpfung:** Es sollte rechtlich klargestellt werden, unter welchen Voraussetzungen KI-Dienste, Suchmaschinen und Plattformen geschützte journalistische Inhalte zusammenfassen, wiedergeben und kommerziell nutzen dürfen. Wo eine Nutzung erlaubnispflichtig ist oder das ursprüngliche Angebot wirtschaftlich weitgehend ersetzt, müssen angemessene Lizenz- und Vergütungsmodelle greifen. Quellen müssen deutlich erkennbar und unmittelbar erreichbar sein.

- **Kennzeichnung und Nachvollziehbarkeit KI-generierter Inhalte:** Immer häufiger werden Inhalte wie Bilder oder Ton- und Videoaufzeichnungen mit Hilfe von künstlicher Intelligenz erstellt oder manipuliert, die das Ziel der Desinformation verfolgen – sogenannte Deepfakes. Bei Deepfakes und genauso bei allen Inhalten von öffentlichem Interesse muss die Erstellung bzw. Bearbeitung mithilfe von KI sichtbar gekennzeichnet werden.⁶²
- **Menschliche Kreativität beim Einsatz von KI schützen:** In Zukunft werden immer mehr Menschen mit KI arbeiten und sie u. a. als Unterstützung ihrer künstlerischen Arbeit nutzen. Dafür muss gewährleistet werden, dass Kreative KI als Werkzeug einsetzen können, ohne den Schutz ihrer eigenen schöpferischen Leistungen zu verlieren. Entscheidend soll und muss dabei der menschliche schöpferische Beitrag sein. Zugleich müssen die Rechte an verwendeten geschützten Werken gewahrt bleiben. Es braucht dementsprechend genaue Vorgaben, in welchem Maße und in welchen Bereichen KI bei der Schaffung neuer Werke genutzt werden darf.

Die Existenzgrundlage künstlerisch-kreativer, journalistisch und wissenschaftlich tätiger Menschen und Organisationen sollte nicht durch generative KI-Modelle gefährdet werden. **Das Urheberrecht muss entsprechend weiterentwickelt und durchgesetzt werden**, um eine möglichst große Transparenz und gleichzeitig sichere und faire Geschäfts- und Vergütungsmodelle zu gewährleisten.

7 WIRKSAME UND UNABHÄNGIGE RECHTSBEHELFE GEGEN PLATTFORMENTSCHEIDUNGEN

Digitale Plattformen sind Legislative, Exekutive und Judikative zugleich: Sie legen ihre eigenen Gemeinschaftsregeln fest, setzen diese Regeln durch und überprüfen vielfach auch Beschwerden gegen ihre eigenen Entscheidungen. Dadurch entsteht eine erhebliche Machtkonzentration. Die Sperrung eines Kontos, die Löschung von Inhalten, eine Einschränkung der Reichweite oder der Ausschluss von der Monetarisierung können die Meinungsfreiheit, gesellschaftliche Teilhabe und wirtschaftliche Existenz der Betroffenen erheblich beeinträchtigen.⁶³

Nutzende benötigen deshalb wirksame Möglichkeiten, Entscheidungen von Plattformen nachvollziehen und unabhängig überprüfen zu lassen. Interne Beschwerdeverfahren allein reichen nicht aus, wenn die Plattform ihre ursprüngliche Entscheidung selbst kontrolliert. Die bereits durch den Digital Services Act vorgesehenen Beschwerde- und Streitbeilegungsverfahren müssen daher konsequent umgesetzt, flächendeckend verfügbar und in ihrer Wirksamkeit gestärkt werden.⁶⁴

Beispiel: Die Influencerin Marie Joan macht Aufklärungsinhalt vor allem für junge Frauen und erreicht mit ihrem Account über 800.000 Menschen. Ihr Kanal wurde im April 2026 ohne Begründung von Meta gesperrt.

Nach einer Welle der Empörung wurde er nach fünf Tagen wieder freigeschaltet.⁶⁵

Solche Fälle zeigen, wie gravierend intransparente Moderationsentscheidungen für Betroffene sein können – insbesondere, wenn sie über Jahre Reichweite, Inhalte und eine berufliche Existenz aufgebaut haben.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Nachvollziehbare Begründungspflichten:** Plattformen müssen Entscheidungen über die Löschung von Inhalten, Kontosperrungen, Reichweitenbeschränkungen, Demonetarisierungen oder vergleichbare Eingriffe konkret und verständlich begründen. Dabei müssen die verletzte Regel, die Gründe, die dem Vorgehen zugrunde liegen, sowie der mögliche Einsatz automatisierter Systeme offengelegt werden.⁶⁶
- **Wirksame interne Beschwerdeverfahren:** Betroffene müssen Plattformentscheidungen einfach, kostenfrei und innerhalb einer angemessenen Frist anfechten können. Die Überprüfung darf bei schwerwiegenden Eingriffen nicht ausschließlich automatisiert erfolgen, sondern muss durch fachlich qualifizierte Personen begleitet werden. Bei vollständigen Kontosperrungen und/oder erheblichen wirtschaftlichen Auswirkungen müssen Eilverfahren möglich sein.⁶⁷

- **Unabhängige Streitbeilegungsstellen:** Zusätzlich zu den internen Verfahren müssen unabhängige und fachkundige Beschwerde- und Berufungsstellen zur Verfügung stehen. Ihre Verfahren müssen barrierearm, leicht auffindbar und für die Betroffenen kostengünstig sein.⁶⁸
- **Stärkere Wirkung unabhängiger Entscheidungen:** Plattformen sollten Entscheidungen anerkannter Streitbeilegungsstellen grundsätzlich umsetzen oder eine Abweichung detailliert und überprüfbar begründen müssen. Wiederholte oder systematische Nichtbefolgung sollte von den zuständigen Aufsichtsbehörden geprüft und gegebenenfalls sanktioniert werden.⁶⁹
- **Sicherung und Portabilität von Inhalten:** Gesperrte Nutzende müssen ihre eigenen Inhalte, Kontakte und Daten weiterhin sichern und exportieren können. Inhalte dürfen während eines laufenden Beschwerdeverfahrens nicht endgültig gelöscht werden, sofern keine zwingenden rechtlichen Gründe entgegenstehen.⁷⁰
- **Transparenz über Moderationsentscheidungen:** Plattformen müssen regelmäßig veröffentlichen, wie viele Inhalte und Konten gesperrt, gelöscht oder in ihrer Reichweite eingeschränkt wurden, welche Gründe dafür ausschlaggebend waren und wie häufig Beschwerden erfolgreich waren. Dadurch können systematische Fehlentscheidungen und diskriminierende Moderationspraktiken erkannt werden.⁷¹
- **Beteiligung von Nutzenden und Zivilgesellschaft:** Nutzende, Wissenschaft, Journalismus und zivilgesellschaftliche Organisationen sollten bei der Weiterentwicklung von Gemeinschaftsregeln, Moderationsstandards und Beschwerdeverfahren angemessen beteiligt werden. Hierfür können unabhängige Beiräte und transparente Konsultationsverfahren eingerichtet werden.^{72, 73}

Beschwerderechte nach dem Digital Services Act:

Der Digital Services Act verpflichtet Online-Plattformen, Entscheidungen über Inhaltslöschungen, Reichweitenbeschränkungen und Kontosperrungen konkret zu begründen. Nutzende können diese Entscheidungen zunächst über ein kostenloses internes Beschwerdeverfahren überprüfen lassen.

Darüber hinaus können sie sich an eine in der Europäischen Union zertifizierte außergerichtliche Streitbeilegungsstelle wenden. Diese Stellen müssen unabhängig, fachkundig, leicht zugänglich und kostengünstig arbeiten. Bislang sind diese Entscheidungen nicht verbindlich.⁷⁴

Wer durch eine Plattformsentscheidung erheblich in seiner Meinungsäußerung, Reichweite oder wirtschaftlichen Tätigkeit betroffen ist, benötigt einen verständlichen, schnellen und unabhängigen Rechtsbehelf. **Digitale Souveränität setzt voraus, dass Plattformen nicht allein über die Regeln, deren Durchsetzung und die Überprüfung ihrer eigenen Entscheidungen bestimmen.** Wirksame Beschwerde- und Berufungsverfahren schaffen Transparenz, schützen die Rechte der Nutzenden und begrenzen die Macht marktprägender Plattformen.



SICHERHEIT

Digitale Infrastrukturen sind eine wesentliche Voraussetzung für die Handlungsfähigkeit von Staat, Wirtschaft und Gesellschaft. Verwaltung, Energieversorgung, Gesundheitswesen, Kommunikation, Finanzsysteme und viele weitere zentrale Bereiche sind heute auf zuverlässige funktionierende digitale Technologien angewiesen. Störungen, Cyberangriffe oder der Ausfall einzelner Anbieter können deshalb weitreichende Folgen für das öffentliche Leben und die wirtschaftliche Stabilität haben.

Gleichzeitig bestehen in vielen sicherheitsrelevanten Bereichen erhebliche Abhängigkeiten von einzelnen amerikanischen und anderen außereuropäischen Technologieanbietern.⁷⁵ Diese Abhängigkeiten können durch politische Konflikte, extraterritoriale Rechtszugriffe, unterbrochene Lieferketten, ausbleibende Sicherheitsupdates oder gezielte Einflussnahme zu einem strategischen Risiko werden. **Digitale Souveränität ist damit zentraler Bestandteil moderner Sicherheits- und Verteidigungspolitik.**

Digitale Souveränität bedeutet in diesem Zusammenhang nicht vollständige technologische Autarkie. Deutschland und Europa müssen jedoch kritische einseitige Abhängigkeiten kennen und reduzieren, belastbare Alternativen aufbauen und ihre Handlungsfähigkeit auch in Krisensituationen erhalten. Sie müssen auch unter veränderten geopolitischen Bedingungen in jedem Fall handlungsfähig bleiben.

SICHERHEIT

- 1 Ressortübergreifende Strategie für digitale Souveränität entwickeln und verbindlich umsetzen
- 2 IT-Sicherheit und Resilienz im Infrastruktur Sondervermögen verbindlich verankern
- 3 Europäische Interessen selbstbewusst vertreten
- 4 Recht auf starke Verschlüsselung sichern und Nutzung konsequent umsetzen
- 5 Kritische Technologieabhängigkeiten staatlicher Sicherheitsbehörden reduzieren

1 RESSORTÜBERGREIFENDE STRATEGIE FÜR DIGITALE SOUVERÄNITÄT ENTWICKELN UND VERBINDLICH UMSETZEN

Digitale Souveränität betrifft zahlreiche Politikfelder gleichzeitig. Sie reicht von Cybersicherheit, öffentlicher Verwaltung und Verteidigung über Wirtschafts- und Industriepolitik bis hin zu Bildung und Außenpolitik. Deutschland benötigt ein gemeinsames und verbindliches Zielbild, das bestehende Aktivitäten zusammenführt, Prioritäten setzt und klare Verantwortlichkeiten festlegt.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Gemeinsame (europäische) Strategie:** Die Bundesregierung muss eine ressortübergreifende Strategie für digitale Souveränität entwickeln, die gemeinsame Ziele und Prioritäten für alle beteiligten Ressorts festlegt. Diese muss eng mit den europäischen Zielen zur Technologiesouveränität und dem Aufbau eines leistungsfähigen European Digital Stack verbunden werden. Nationale Maßnahmen sollten europäische Lösungen stärken und keine unnötigen Parallelstrukturen schaffen.⁷⁶
- **Verbindliche politische Verantwortung und Zuständigkeit:** Die Strategie sollte vom Bundeskabinett beschlossen und unter Beteiligung des Bundeskanzleramts sowie aller relevanten Ressorts umgesetzt werden. Jede Maßnahme muss in der klaren Zuständigkeit eines Ressorts und beteiligter Behörden liegen.⁷⁷
- **Bestandsaufnahme kritischer Abhängigkeiten:** Deutschland muss systematisch erfassen, in welchen Bereichen besonders kritische einseitige Abhängigkeiten bestehen. Auf dieser Grundlage soll das Bundesministerium für Digitales und Staatsmodernisierung unter Beteiligung des Bundesamts für Sicherheit in der Informationstechnik eine für die Bundesverwaltung verbindliche und regelmäßig aktualisierte Risiko- und Ausschlussliste erstellen. Dabei sollten sowohl technische als auch wirtschaftliche, rechtliche und geopolitische Risiken berücksichtigt werden.⁷⁸
- **Einbindung relevanter Akteure:** Die Strategie muss festlegen, welche Technologien und Fähigkeiten national, europäisch oder gemeinsam mit vertrauenswürdigen internationalen Partnern aufgebaut und dauerhaft gesichert werden sollen. Darüber hinaus müssen Länder, Kommunen, Wirtschaft, Wissenschaft und Zivilgesellschaft in die Entwicklung und Umsetzung der Strategie einbezogen werden.
- **Finanzierung und Planung:** Die Strategie muss mit einer verlässlichen Finanzierung und konkreten Meilensteinen hinterlegt werden und darf nicht von wechselnden Förderprogrammen abhängen. Fortschritte müssen anhand geeigneter Indikatoren regelmäßig überprüft und transparent veröffentlicht werden. Für besonders kritische digitale Dienste müssen zusätzlich Notfall-, Migrations- und Exit-Strategien entwickelt werden, damit staatliche Stellen handlungsfähig bleiben, wenn ein Anbieter ausfällt, seine Leistungen einstellt oder nicht mehr zuverlässig genutzt werden kann.

Nur durch eine langfristige und ressortübergreifende Strategie können Deutschland und Europa kritische Abhängigkeiten systematisch reduzieren und ihre digitale Handlungsfähigkeit dauerhaft sichern.

2 IT-SICHERHEIT UND RESILIENZ IM INFRASTRUKTUR SONDERVERMÖGEN VERBINDLICH VERANKERN

Digitale Infrastruktur ist nur dann zukunftsfähig, wenn ihre Sicherheit, Wartbarkeit und Krisenfestigkeit von Beginn an mitgedacht werden. Ohne ausreichende Absicherung schafft sie Verwundbarkeiten und kann bestehende Risiken sogar vergrößern. Investitionen in neue digitale Infrastrukturen müssen deshalb immer auch die notwendigen Sicherheitsmaßnahmen umfassen.

Das Sondervermögen für Infrastruktur und Klimaneutralität bietet diese Chance, doch: IT-Sicherheit darf dabei nicht als nachträgliche Zusatzaufgabe verstanden werden, sondern muss integraler Bestandteil der Investitionen sein.⁷⁹ *Die Relevanz muss sich in der Finanzierung angemessen widerspiegeln.*

2025 wurde das mehrjährige **Investitionspaket Sondervermögen Infrastruktur und Klimaneutralität (SVIK)** über 500 Milliarden Euro beschlossen. Davon fließen 300 Mrd. in Infrastrukturmaßnahmen der Bundesregierung, 100 Mrd. bekommen Länder und Kommunen und weitere 100 Mrd. sollen den Klima- und Transformationsfonds stärken. Wenn man sich die Aufteilung der Bereiche anschaut, in die das Geld fließen soll, wird anhand der Wirtschaftspläne 2025/26⁸⁰ deutlich, dass zwar einiges in die Digitalisierung investiert wird – aber der Bereich der digitalen Sicherheit wird hierbei nicht klar definiert oder gar priorisiert.⁸¹

Wir schlagen deshalb folgende Maßnahmen vor:

- **Verbindliche Sicherheits- und Resilienzkriterien:** Aus dem Sondervermögen finanzierte Digitalisierungsprojekte müssen verbindliche Anforderungen an IT-Sicherheit, Wartbarkeit, Notfallfähigkeit und Resilienz erfüllen. Diese müssen bereits bei Planung und Beschaffung berücksichtigt und für die Umsetzung müssen ausreichende und verbindlich ausgewiesene Mittel vorgesehen werden. Die Wirkung der Investitionen muss anhand konkreter Sicherheits- und Resilienzindikatoren regelmäßig überprüft werden.⁸²
- **Modernisierung kritischer Altsysteme und Aufbau sicherer Basisstrukturen:** Investitionen sollten sich auf die Ablösung oder Absicherung veralteter und nicht mehr zuverlässig wartbarer IT-Systeme sowie auf sichere Rechenzentren und Netze, Identitäts- und Zugriffsmanagement, Verschlüsselungs-, Backup- und Wiederherstellungsinfrastrukturen und Fähigkeiten zur Angriffserkennung und -abwehr konzentrieren.⁸³
- **Langfristigkeit:** Bereits bei Investitionsentscheidungen müssen Sicherheitsupdates, Wartung, Support, Wiederherstellbarkeit und Exit-Strategien über den gesamten Lebenszyklus einer Technologie berücksichtigt werden. Systeme dürfen nicht aufgebaut werden, ohne ihre langfristige sichere Betriebsfähigkeit sicherzustellen.⁸⁴
- **Unterstützung für Länder und Kommunen:** Länder, Kommunen und andere öffentliche Einrichtungen benötigen neben finanziellen Mitteln auch zentrale Beratung, Referenzarchitekturen, gemeinsame Beschaffungsmöglichkeiten und leicht nutzbare Sicherheitsangebote.

Digitalisierung und IT-Sicherheit dürfen nicht getrennt voneinander betrachtet werden. **Investitionen aus dem SVIK** müssen deshalb dazu beitragen, nicht nur mehr digitale Infrastruktur aufzubauen, sondern diese auch sicher, resilient und langfristig beherrschbar zu gestalten.

3 EUROPÄISCHE INTERESSEN SELBSTBEWUSST VERTRETEN

Technologische Abhängigkeiten sind nicht nur eine wirtschaftliche, sondern auch eine sicherheits- und außenpolitische Frage. Wenn zentrale digitale Infrastrukturen von einzelnen Unternehmen oder Drittstaaten abhängig sind, entstehen strukturelle Machtasymmetrien. Europa muss deshalb in der Lage sein, seine technologischen und sicherheitspolitischen Interessen eigenständig zu definieren und konsequent zu vertreten.

Eine partnerschaftliche Zusammenarbeit mit den USA und weiteren internationalen Partnern bleibt dabei wichtig. Sie darf jedoch nicht mit einseitiger Abhängigkeit verwechselt werden. Gute Partnerschaften setzen eigene Handlungsfähigkeit voraus.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Geschlossenes europäisches Auftreten:** Die Europäische Union sollte ihre technologischen und sicherheitspolitischen Interessen geschlossen vertreten. Dabei dürfen nationale Einzelinteressen die gemeinsame Verhandlungsmacht nicht schwächen. Europäische Regelungen müssen gegenüber allen Unternehmen konsequent angewendet werden und dürfen nicht aus wirtschaftlicher oder außenpolitischer Rücksichtnahme abgeschwächt werden.⁸⁶
- **Europäische Verhandlungsmacht stärken:** Öffentliche Beschaffung, gemeinsame Investitionen und europäische Industriepolitik sollten gezielt genutzt werden, um Europas Position gegenüber marktbeherrschenden Technologieanbietern zu verbessern und einseitige Abhängigkeiten zu reduzieren.⁸⁷
- **Technologiepolitik als Bestandteil der Außen- und Sicherheitspolitik:** Strategisch relevante Technologien wie Cloud-Infrastrukturen, Halbleiter, Künstliche Intelligenz, Kommunikationssysteme und Cybersicherheit müssen systematisch in außen-, handels- und sicherheitspolitische Entscheidungen einbezogen werden.^{88, 89}
- **Abhängigkeiten diversifizieren:** Europa sollte kritische technologische Abhängigkeiten nicht lediglich von einem Anbieter oder Staat auf einen anderen verlagern. Eigene europäische Fähigkeiten müssen durch belastbare Zusammenarbeit mit vertrauenswürdigen internationalen Partnern ergänzt werden.

Die Anwendung europäischen Rechts und die Wahrung strategischer Interessen dürfen nicht davon abhängen, ob ihre Durchsetzung außenpolitisch unbequem ist. Europa braucht keine technologische Abschottung, sondern eigene Handlungsfähigkeit. Partnerschaften mit Drittstaaten müssen auf Augenhöhe stattfinden und dürfen nicht auf struktureller Abhängigkeit beruhen.

4 RECHT AUF STARKE VERSCHLÜSSELUNG SICHERN UND IHRE NUTZUNG KONSEQUENT UMSETZEN

Starke Verschlüsselung ist eine zentrale Voraussetzung moderner IT-Sicherheit und unverzichtbar für den Schutz digitaler Informationen.⁹⁰ Dabei müssen zwei Ziele gemeinsam verfolgt werden: Einerseits darf starke Verschlüsselung nicht politisch oder technisch systematisch geschwächt werden. Andererseits muss moderne Kryptografie insbesondere in kritischen und sensiblen Bereichen konsequent und fachgerecht eingesetzt werden. Ein Recht auf starke Verschlüsselung und ihre praktische Umsetzung gehören deshalb zusammen.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Recht auf starke Verschlüsselung:** Bürgerinnen und Bürger, Unternehmen sowie öffentliche Einrichtungen müssen starke Verschlüsselung und insbesondere Ende-zu-Ende-Verschlüsselung einsetzen dürfen. Dieses Recht darf insbesondere nicht durch verpflichtende Hintertüren, General-schlüssel oder vergleichbare technische Zugriffsmöglichkeiten ausgehöhlt werden.⁹¹
- **Konsequenter Einsatz in kritischen Bereichen:** Sensible und kritische Daten müssen entsprechend ihrer Schutzbedürftigkeit bei der Übertragung und Speicherung verschlüsselt werden. In besonders schutzwürdigen Bereichen sollte zudem geprüft werden, ob zusätzliche kryptografische Schutzmaßnahmen während der Verarbeitung erforderlich und technisch sinnvoll sind.⁹²
- **NIS2 und DORA konsequent umsetzen:** Die bereits bestehenden europäischen Anforderungen an Kryptografie und Verschlüsselung müssen in den betroffenen Organisationen konsequent umgesetzt und wirksam kontrolliert werden. NIS2 und DORA zeigen, dass Verschlüsselung inzwischen als zentraler Bestandteil eines angemessenen Cyberrisikomanagements anerkannt ist.^{93, 94}
- **Sicheres Schlüsselmanagement:** Wirksame Verschlüsselung setzt ein professionelles Schlüsselmanagement nach klaren Sicherheitsstandards voraus.
- **Krypto-Agilität und Post-Quantum-Migration:** Kritische Systeme müssen so ausgelegt sein, dass kryptografische Verfahren bei neuen Bedrohungen oder technologischen Entwicklungen ausgetauscht und regelmäßig an den Stand der Technik angepasst werden können. Organisationen müssen ihre eingesetzte Kryptografie inventarisieren, quanten-verwundbare Verfahren identifizieren und konkrete Migrationspläne entwickeln. Die Umstellung auf post-quanten-sichere Verfahren – also auf kryptografische Verfahren, die nach heutigem Kenntnisstand auch Angriffen leistungsfähiger Quantencomputer standhalten – ist insbesondere bei kritischen, langlebigen und besonders schutzwürdigen Systemen prioritär voranzutreiben. Neue Systeme und Beschaffungen müssen von Beginn an krypto-agil und für den Einsatz post-quanten-sicherer Verfahren ausgelegt sein.^{95, 96}

Starke Verschlüsselung ist eine zentrale Voraussetzung für digitale Sicherheit. Digitale Souveränität setzt voraus, dass Menschen und Organisationen ihre Kommunikation und Daten wirksam schützen können.



KRITISCHE TECHNOLOGIEABHÄNGIGKEITEN STAATLICHER SICHERHEITSBEHÖRDEN REDUZIEREN

Staatliche Sicherheitsbehörden, Bundeswehr und andere besonders sicherheitsrelevante Einrichtungen stellen höchste Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit ihrer digitalen Systeme. Für diese Bereiche reicht es jedoch nicht aus, allein den Schutz der verarbeiteten Daten zu betrachten.

Ein anschauliches Beispiel ist die Integration von Google Cloud Air-Gapped in die Multi-Cloud-Infrastruktur der Bundeswehr.

Wie im Mai 2025 bekanntgegeben wurde, setzt die deutsche Bundeswehr für ihre eigene Cloud mit hochsensiblen Daten auf eine Lösung von Google. Die Lösung wird zwar physisch getrennt von anderen Google-Systemen und -Netzwerken betrieben, und Softwareupdates werden über physische Datenträger aufgespielt. Dennoch bleibt der eingesetzte Software-Stack einschließlich Pflege und Weiterentwicklung ein Produkt eines US-amerikanischen Herstellers. Damit bestehen trotz eigener Kontrolle über Betrieb und Daten weiterhin technologische Herstellerabhängigkeiten.

Die Bundeswehr verfolgt deshalb bereits einen Multi-Cloud-Ansatz mit mehreren unterschiedlichen Cloud-Lösungen, darunter auch eine Open-Source-basierte Alternative.⁹⁷

Das Beispiel verdeutlicht: Datensouveränität allein bedeutet noch keine vollständige Technologiesouveränität. Auch bei einem vollständig selbst betriebenen System können Abhängigkeiten hinsichtlich Softwarepflege, Sicherheitsupdates, technischer Weiterentwicklung, Support oder Lizenzierung bestehen.

Die Herkunft einer Technologie darf nicht mit ihrer technischen Sicherheit gleichgesetzt werden. Auch europäische oder quelloffene Lösungen können Schwachstellen enthalten; bei Technologien aus Drittstaaten können jedoch zusätzliche rechtliche, geopolitische und herstellerbezogene Risiken entstehen. Solche Abhängigkeiten sind nicht automatisch ein Sicherheitsrisiko, müssen bei besonders kritischen staatlichen Systemen aber systematisch bewertet und begrenzt werden.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Höhere Souveränitätsanforderungen für sicherheitskritische Systeme:** Je kritischer ein staatliches System für Sicherheit und Handlungsfähigkeit ist, desto höher müssen die Anforderungen an technische Kontrolle, Auditierbarkeit, eigene Betriebsfähigkeit und Herstellerunabhängigkeit sein. Sowohl bestehende als auch neu entstehende Abhängigkeiten müssen nach technischer Sicherheit, Softwarepflege und geopolitischen Risiken regelmäßig bewertet werden.⁹⁸
- **Europäische und offene Alternativen:** Für strategisch besonders relevante Technologien müssen leistungsfähige europäische und Open-Source-basierte Alternativen gezielt entwickelt, finanziert und eingesetzt werden. Ziel ist nicht ein kurzfristiger Austausch funktionierender Systeme, sondern der langfristige Aufbau echter Wahlmöglichkeiten.

- **Anbieterabhängigkeit vermeiden und Exit-Fähigkeit sichern:** Kritische Systeme sollten nicht unnötig von einzelnen Anbietern abhängig sein. Offene Standards, Multi-Vendor- und Multi-Cloud-Strategien sowie verbindliche Exit- und Migrationsstrategien müssen einen Anbieterwechsel ermöglichen.^{99, 100}
- **Software-Supply-Chain absichern:** Bei sicherheitskritischer Software müssen Herkunft und Zusammensetzung der eingesetzten Komponenten nachvollziehbar sein. Dazu gehören insbesondere Software Bill of Materials (SBOM), sichere und signierte Updateverfahren, Schwachstellenmanagement sowie unabhängige Sicherheitsprüfungen. BSI und ZenDiS haben sichere Softwarelieferketten ausdrücklich als Bestandteil souveräner digitaler Infrastruktur eingeordnet; auch der Cyber Resilience Act stärkt unter anderem SBOM und Schwachstellenmanagement.¹⁰¹
- **Eigenes technisches Know-how:** Sicherheitsbehörden müssen ausreichend eigene Kompetenzen besitzen, um kritische Systeme bewerten, betreiben und deren Sicherheit kontrollieren zu können. **Kernkompetenzen dürfen nicht vollständig an externe Hersteller oder Dienstleister ausgelagert werden.**

Wenn der Angriff über den Softwarelieferanten kommt – SolarWinds

Der SolarWinds-Hack zeigt exemplarisch, warum Softwarelieferketten selbst zu einem Sicherheitsrisiko werden können. Angreifer kompromittierten die Lieferkette der weit verbreiteten Netzwerkmanagementsoftware SolarWinds Orion und schleusten Schadcode über manipulierte Softwareupdates in Systeme von Kunden ein. Die US-Cybersicherheitsbehörde CISA warnte im Dezember 2020 vor der aktiven Ausnutzung betroffener Orion-Versionen und ordnete den Vorfall später ausdrücklich als Kompromittierung einer Software-Supply-Chain ein. Betroffen waren zahlreiche Unternehmen und US-Regierungsstellen. Auch verschiedene deutsche Behörden hatten SolarWinds-Produkte im Einsatz, wobei dies nicht automatisch bedeutete, dass deren Systeme tatsächlich kompromittiert worden waren.

Der Fall verdeutlicht ein grundsätzliches Problem: Selbst gut abgesicherte Organisationen vertrauen darauf, dass Software und Updates ihrer Lieferanten integer sind. Wird diese Vertrauensbeziehung kompromittiert, kann gerade ein regulärer und eigentlich vertrauenswürdiger Updateprozess zum Angriffsweg werden. Sichere Softwarelieferketten, nachvollziehbare Komponenten, überprüfbare Updates und die Fähigkeit zur unabhängigen Sicherheitsbewertung sind deshalb wesentliche Bestandteile digitaler Souveränität.¹⁰²

Für sicherheitskritische staatliche Systeme reicht es nicht, dass Daten unter eigener Kontrolle bleiben. Digitale Souveränität setzt voraus, dass auch Betrieb, Weiterentwicklung und ein möglicher Wechsel langfristig beherrschbar bleiben. Ziel ist keine vollständige technologische Autarkie, sondern die **Fähigkeit, auch unter veränderten politischen, wirtschaftlichen oder technischen Rahmenbedingungen selbstbestimmt handlungsfähig zu bleiben.**



WIRTSCHAFT

Digitale Technologien sind heute eine zentrale Grundlage wirtschaftlicher Wertschöpfung. Cloud-Infrastrukturen, Softwareplattformen, Datenräume, Kommunikationsdienste und KI-Systeme prägen zunehmend die Wettbewerbsfähigkeit von Unternehmen. Gleichzeitig werden aktuell wesentliche Teile dieser digitalen Infrastruktur von wenigen globalen Technologieunternehmen kontrolliert. Dadurch entstehen insbesondere für europäische Unternehmen strukturelle Abhängigkeiten.

Diese Abhängigkeiten wirken sich bereits im normalen Wirtschaftsbetrieb aus (z. B. durch Vendor Lock-in, geringe Verhandlungsmacht, eingeschränkte Datenportabilität) und bedeuten in geopolitischen oder wirtschaftlichen Krisensituationen zusätzlich erhebliche Risiken für die wirtschaftliche Handlungsfähigkeit.¹⁰³

Ein digitaler Blackout muss dabei nicht bedeuten, dass sämtliche digitalen Dienste gleichzeitig ausfallen. Bereits die kurzfristige Einschränkung oder der Entzug des Zugangs zu strategisch wichtigen Cloud-, Software-, Plattform- oder KI-Diensten kann Unternehmen und ganze Wertschöpfungsketten erheblich beeinträchtigen. Je stärker zentrale Geschäftsprozesse von wenigen extern kontrollierten Technologien abhängen, desto größer sind die möglichen wirtschaftlichen Folgen.¹⁰⁴

Digitale Souveränität ist damit auch Wirtschafts-, Innovations- und Standortpolitik. Ziel ist nicht technologische Abschottung, sondern der Aufbau eigener Kompetenzen, leistungsfähiger Alternativen und belastbarer Wechselemöglichkeiten bei strategisch wichtigen Technologien.

WIRTSCHAFT

- 1 KRITIS: verbindliche Souveränitätsanforderungen für kritische digitale Technologien
- 2 Open Source stärken
- 3 Transfer- und Vernetzungsstrukturen schaffen
- 4 Marktzugang setzt die Einhaltung europäischen Rechts voraus
- 5 Öffentliches und institutionelles Kapital für europäische Schlüsseltechnologien mobilisieren

1 KRITIS: VERBINDLICHE SOUVERÄNITÄTSANFORDERUNGEN FÜR KRITISCHE DIGITALE TECHNOLOGIEN

Kritische Infrastrukturen wie Energie- und Wasserversorgung, Verkehr, Gesundheitswesen oder Telekommunikation sind für die Funktionsfähigkeit von Wirtschaft und Gesellschaft unverzichtbar, und ihr Schutz eine der Kernaufgaben staatlicher und unternehmerischer Sicherheitsvorsorge. Entsprechend hoch sind die Anforderungen an ihre Sicherheit und Resilienz. Neben dem Schutz vor Cyberangriffen muss dabei berücksichtigt werden, von welchen Herstellern, Technologien und digitalen Diensten der Betrieb kritischer Funktionen langfristig abhängt. Dabei ist nicht jede IT-Komponente eines KRITIS-Unternehmens gleichermaßen kritisch. Entscheidend sind insbesondere Systeme und Dienste, deren Ausfall, Manipulation oder Entzug die Erbringung einer kritischen Dienstleistung wesentlich beeinträchtigen könnte.¹⁰⁵

Souveränität darf dabei nicht allein anhand des Sitzes eines Herstellers bewertet werden. Entscheidend ist, in welchem Umfang Daten, Betrieb, Softwarelieferketten, technische Weiterentwicklung und ein möglicher Anbieterwechsel tatsächlich kontrollierbar sind. Je kritischer eine digitale Funktion ist, desto höher müssen die verbindlichen Anforderungen an diese technologische Souveränität sein. Für besonders kritische Funktionen kann daraus auch die Anforderung entstehen, dass wesentliche operative und technologische Kontrolle innerhalb Europas liegen muss.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Europäische Strategie abstimmen:** Die Entwicklung souveräner Technologien für kritische Infrastrukturen sollte eng mit der europäischen Technologiesouveränitätspolitik und der weitergehenden Vision eines europäischen Digital Stack beziehungsweise EuroStack verzahnt werden. Verbindliche und langfristig planbare Souveränitätsanforderungen schaffen Nachfrage nach europäischen Cloud-Diensten, Rechenzentren, Netzwerktechnologien, Softwareplattformen, Datenräumen, Cybersecurity-Lösungen und KI-Systemen.¹⁰⁶
- **Verbindliche und überprüfbare Souveränitätsanforderungen:** Für digitale Systeme und Komponenten, die für die Erbringung kritischer Dienstleistungen wesentlich sind, müssen neben klassischen Sicherheitsanforderungen verbindliche Kriterien für technologische Souveränität definiert werden. Dazu gehören insbesondere rechtliche und jurisdiktionelle Kontrolle, Datenkontrolle, Auditierbarkeit, Wartbarkeit, Softwarelieferketten sowie Wechsel- und Exit-Fähigkeit.¹⁰⁷
- **Kritikalität bestimmt das Souveränitätsniveau:** Die Anforderungen müssen risikobasiert gestaffelt werden. Je größer die Auswirkungen eines Ausfalls, einer Manipulation oder eines externen Zugriffs- oder Lieferstopps wären, desto höher müssen die Anforderungen an eigene Kontrolle, Herstellerunabhängigkeit und europäische Handlungsfähigkeit sein. Bei besonders kritischen Funktionen sollten Betrieb und Kontrolle innerhalb Europas liegen und Softwarelieferketten möglichst umfassend nachvollziehbar sein. Kritische einseitige Abhängigkeiten von einzelnen Drittstaaten oder Herstellern müssen vermieden oder systematisch reduziert werden.¹⁰⁸

- **Bestehende KRITIS- und NIS2-Regelungen weiterentwickeln:** Die bestehenden Anforderungen an Sicherheit, Resilienz und Lieferketten sollten um konkrete Souveränitätsanforderungen für besonders kritische digitale Systeme und Komponenten ergänzt und in technischen Vorgaben sowie bei Beschaffungsentscheidungen operationalisiert werden. Für Neubeschaffungen müssen verbindliche Mindestanforderungen an technologische Souveränität gelten. Für bestehende kritische Abhängigkeiten sind Migrationspläne und realistische Zieltermine für deren Reduzierung festzulegen.
- **Exit-Fähigkeit:** Kritische Infrastrukturen dürfen nicht dauerhaft von einem einzelnen Technologieanbieter abhängig werden. Offene Schnittstellen, portable Daten, dokumentierte Migrationspfade und verfügbare Alternativen müssen einen Anbieterwechsel ermöglichen.¹⁰⁹

Die Sicherung kritischer Infrastrukturen ist damit nicht nur eine Aufgabe der Cybersecurity, sondern auch der Wirtschafts- und Industriepolitik. **Verbindliche Souveränitätsanforderungen können kritische Abhängigkeiten reduzieren und gleichzeitig einen verlässlichen europäischen Markt für sichere und souveräne digitale Technologien schaffen.** Ziel ist nicht technologische Abschottung, sondern die Fähigkeit, kritische Dienstleistungen auch bei sich verändernden Rahmenbedingungen sicher aufrechterhalten zu können.

2 OPEN SOURCE STÄRKEN

Open Source ist eine wichtige Grundlage digitaler Souveränität. Offener Quellcode ermöglicht es, Software unabhängig zu prüfen, anzupassen, selbst zu betreiben und bei Bedarf weiterzuentwickeln. Dadurch können technologische Abhängigkeiten und Vendor Lock-in reduziert und langfristige Wahlmöglichkeiten geschaffen werden.

Er allein garantiert jedoch noch keine digitale Souveränität. Open-Source-Lösungen müssen funktional wettbewerbsfähig, sicher, benutzbar, integrierbar und wirtschaftlich tragfähig sein. Für Unternehmen zählen insbesondere einfache Migration, verlässliche Sicherheitsupdates, professioneller Support und langfristige Wartbarkeit. Nur dann werden offene Lösungen zu attraktiven Alternativen zu etablierten proprietären Angeboten.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Open-Source-Förderung langfristig ausbauen:** Bund und Europäische Union sollten Förderprogramme für strategisch relevante Open-Source-Technologien verstetigen und ausweiten. Bestehende Ansätze wie der Sovereign Tech Fund und die EU-Strategie für offene digitale Ökosysteme bieten dafür wichtige Grundlagen. Förderfähig sein müssen nicht nur neue Funktionen, sondern auch Wartung, Sicherheitsupdates, Tests, Dokumentation, Release-Management und Community-Arbeit.^{110, 111}
- **Produktreife gezielt stärken:** Open-Source-Projekte müssen dabei unterstützt werden, von vielversprechenden Ansätzen aus der Forschung oder technisch leistungsfähigen Lösungen zu professionell einsetzbaren Produkten und Plattformen zu werden. Dazu gehören beispielsweise die einfache Installation und Migration oder die Integration in bestehende Systeme.
- **Usability als Förderziel:** Gebrauchstauglichkeit muss bei der Entwicklung souveräner Alternativen von Anfang an mitgedacht werden. Intuitive Bedienung, verständliche Sicherheits- und Datenschutzeinstellungen sowie barrierearme Nutzung können entscheidend dafür sein, ob Organisationen tatsächlich zu offenen Lösungen wechseln.
- **Sichere Open-Source-Infrastruktur:** Besonders verbreitete Open-Source-Lösungen wie Bibliotheken, Paketmanager, Frameworks, kryptografische Komponenten und andere digitale Basistechnologien müssen als kritische Infrastruktur der Softwarewirtschaft betrachtet und entsprechend unterstützt werden.¹¹²
- **Nachhaltige Geschäftsmodelle fördern:** Förderprogramme sollten gezielt Unternehmen unterstützen, die auf Basis von Open Source tragfähige Geschäftsmodelle entwickeln – beispielsweise durch Hosting, Managed Services, Support, Integration, Beratung, Security Services oder branchenspezifische Weiterentwicklungen.¹¹³
- **Förderung mit öffentlicher Beschaffung verbinden:** Staatliche Förderung allein schafft noch keinen nachhaltigen Markt. Öffentliche Einrichtungen und Unternehmen sollten zusätzlich leistungsfähige Open-Source-Lösungen stärker nachfragen und so Referenzmärkte für europäische Anbieter schaffen.

Open Source wird dann zu einem wirksamen Instrument digitaler Souveränität, **wenn aus offenem Quellcode dauerhaft tragfähige technologische Ökosysteme entstehen**. Europa braucht deshalb nicht nur mehr Open-Source-Projekte, sondern sichere, benutzbare und wirtschaftlich erfolgreiche offene Technologien sowie Unternehmen und Communities, die diese langfristig weiterentwickeln können. Open-Source-Software-Lösungen sollten zukünftig nicht nur durch eine Minderheit aus Überzeugung genutzt werden, sondern attraktive Alternativen darstellen.



TRANSFER- UND VERNETZUNGSSTRUKTUREN SCHAFFEN

Viele Unternehmen haben die Bedeutung digitaler Souveränität erkannt. In der praktischen Umsetzung fehlt jedoch häufig die Orientierung: Welche technologischen Abhängigkeiten sind für das eigene Unternehmen tatsächlich kritisch? Welche Alternativen existieren? Wie lassen sich deren Sicherheit, Wirtschaftlichkeit und Souveränität bewerten? Und wie kann eine Migration umgesetzt werden, ohne laufende Geschäftsprozesse zu gefährden?

Digitale Souveränität ist deshalb nicht nur eine Frage verfügbarer Technologien, sondern auch des Wissens- und Technologietransfers. Unternehmen benötigen anbieterneutrale Anlaufstellen, die sie dabei unterstützen, Abhängigkeiten zu erkennen, geeignete Alternativen zu bewerten, neue Technologien praktisch zu erproben und konkrete Transformationsschritte umzusetzen. Dafür müssen Wissenschaft, Technologieanbieter, Anwenderunternehmen und Transferorganisationen stärker miteinander vernetzt werden.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Digitale Souveränität in bestehende Transferstrukturen integrieren:** Bestehende Netzwerke und Kompetenzstrukturen wie Mittelstand-Digital-Zentren, European Digital Innovation Hubs,¹¹⁴ Kammern, Verbände, Hochschulen, Forschungseinrichtungen und regionale Innovationsnetzwerke sollten digitale Souveränität systematisch als Querschnittsthema aufnehmen. Erfolgreiche Transferstrukturen sollten langfristig finanziert werden und Unternehmen dauerhaft als verlässliche Ansprechpartner zur Verfügung stehen.
- **Anbieterneutrale Beratung und Souveränitätschecks:** Unternehmen benötigen unabhängige Orientierung zu technologischen Abhängigkeiten, Cloud-, Software- und Datenraumlösungen, Open Source, Datenportabilität, Exit-Strategien, Cybersicherheit und souveräner Beschaffung. Die Beratung muss sich an den konkreten Anforderungen des jeweiligen Unternehmens orientieren und darf nicht an einzelnen Produkten oder Anbietern geleitet sein. Ergänzend sollen Souveränitätschecks dabei helfen, bestehende Abhängigkeiten zu erfassen, nach Kritikalität zu bewerten und konkrete Prioritäten und Maßnahmen abzuleiten.¹¹⁵
- **„Test before invest“ ermöglichen:** Unternehmen sollten souveräne Lösungen vor einer Investitionsentscheidung praktisch erproben können, um Funktionalität, Integrationsfähigkeit, Migrationsaufwand und Wirtschaftlichkeit realistisch einschätzen zu können. Auch (branchenspezifische) Praxiserfahrungen helfen dabei.¹¹⁶
- **Anwender, Anbieter und Wissenschaft zusammenbringen:** Geförderte Matchmaking- und Transferformate sollten Unternehmen mit europäischen Technologieanbietern, Open-Source-Communities und Forschungseinrichtungen vernetzen. So können konkrete Anforderungen der Anwender schneller in die Weiterentwicklung souveräner Technologien einfließen.¹¹⁷

- **Pilot- und Migrationsprojekte:** Förderprogramme sollten neben Beratung und Erprobung auch Machbarkeitsstudien, Migrationskonzepte, Pilotierungen und erste Umsetzungsprojekte finanzieren. Insbesondere KMU benötigen technische, organisatorische und finanzielle Unterstützung, um den Wechsel zu souveränen Lösungen ohne Gefährdung laufender Geschäftsprozesse bewältigen zu können.
- **KMU besonders unterstützen:** Kleine und mittlere Unternehmen verfügen häufig nicht über eigene spezialisierte IT-, Security- oder Architekturteams. Beratungs-, Test- und Transferangebote müssen deshalb niedrigschwellig, regional erreichbar und auf die begrenzten personellen und finanziellen Ressourcen von KMU zugeschnitten sein.¹¹⁸
- **Wissenschaft als neutraler Transferpartner:** Hochschulen und Forschungseinrichtungen können Technologien unabhängig evaluieren, Vergleichskriterien entwickeln, Demonstratoren bereitstellen und Unternehmen bei Architektur-, Sicherheits- und Transformationsfragen unterstützen. Diese Transferfunktion sollte gezielt gefördert werden.

Förderprogramme zur digitalen Souveränität sollten somit nicht nur die Entwicklung neuer Technologien unterstützen, sondern auch deren Weg in die praktische Anwendung. Erst wenn Unternehmen Abhängigkeiten erkennen, Alternativen finden, diese erproben und konkrete Migrationschritte umsetzen können, entsteht **aus technologischer Vielfalt tatsächlich wirtschaftliche Handlungsfähigkeit**.

Ziel muss ein **breites Netzwerk aus Technologie- und Open-Source-Communities, Start-ups, KMU, Forschungseinrichtungen und etablierten Technologieunternehmen** sein, das souveräne Technologien entwickelt, betreibt und wirtschaftlich weiterentwickelt.

4 MARKTZUGANG SETZT DIE EINHALTUNG EUROPÄISCHEN RECHTS VORAUS

Der europäische Binnenmarkt bietet Unternehmen Zugang zu einem der größten und wirtschaftlich attraktivsten Märkte der Welt. Wer auf diesem Markt tätig ist, muss im Gegenzug die demokratisch beschlossenen europäischen Regeln einhalten.

Gerade bei marktmächtigen digitalen Unternehmen besteht die Gefahr, dass Sanktionen für Rechtsverstöße lediglich als kalkulierbare Geschäftskosten betrachtet werden.¹¹⁹ Wenn Unternehmen durch Nicht-Compliance wirtschaftliche Vorteile erzielen können, benachteiligt das jene, die in regulatorische Anforderungen, etwa Datenschutz und Cybersicherheit, investieren. Die konsequente Durchsetzung europäischen Rechts ist deshalb nicht nur eine rechtsstaatliche, sondern auch eine wirtschaftspolitische Voraussetzung für fairen Wettbewerb.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Gleiche Regeln für alle Marktteilnehmer:** Unternehmen, die Produkte und Dienstleistungen auf dem europäischen Markt anbieten, müssen europäische Vorgaben einhalten – unabhängig von Herkunftsland oder wirtschaftlicher Bedeutung.
- **Rechtsbruch darf sich wirtschaftlich nicht lohnen:** Sanktionen müssen so bemessen sein, dass die erwartbaren wirtschaftlichen Vorteile eines Regelverstosses nicht höher sind als dessen Konsequenzen. Insbesondere bei marktmächtigen Unternehmen müssen deshalb umsatzbezogene Sanktionen konsequent eingesetzt werden können.
- **Stufenweise Eskalation bei wiederholten Verstößen:** Auf festgestellte Verstöße müssen zunächst Abhilfemaßnahmen und ggf. Zwangsgelder folgen. Bei wiederholter/systematischer Nicht-Compliance müssen im Rahmen der einschlägigen europäischen Rechtsakte auch weitergehende verhaltensbezogene und strukturelle Maßnahmen möglich sein, soweit diese erforderlich/verhältnismäßig sind. Dazu kann bei marktmächtigen Unternehmen als äußerstes strukturelles Mittel auch die organisatorische oder wirtschaftliche Trennung bestimmter Geschäftsbereiche gehören.^{120, 121}
- **Marktzugang als Ultima Ratio beschränken:** Missachtet ein Unternehmen/konkreter Dienst trotz wiederholter Sanktionen und rechtskräftiger Entscheidungen systematisch europäisches Recht, muss als äußerstes Mittel auch eine zeitweise oder – in besonders schwerwiegenden Fällen – dauerhafte Beschränkung auf dem europäischen Markt möglich sein.
- **Verhältnismäßigkeit:** Je schwerwiegender eine Sanktion ist, desto höher müssen die Anforderungen an Begründung, Verhältnismäßigkeit und gerichtliche Überprüfbarkeit sein. Ein Ausschluss vom Markt darf kein politisches Druckmittel, sondern ausschließlich das Ergebnis eines transparenten rechtsstaatlichen Verfahrens sein.¹²²

Der europäische Binnenmarkt ist kein rechtsfreier Raum. Marktmächtige Unternehmen dürfen Verstöße nicht lediglich als Kostenfaktor einkalkulieren. Wer in Europa wirtschaftet, profitiert von einem gemeinsamen Markt und stabilen Rechtsrahmen. Im Gegenzug muss die Einhaltung seiner Regeln selbstverständlich sein. **Rechtsbruch darf kein Wettbewerbsvorteil sein.**

5 ÖFFENTLICHES UND INSTITUTIONELLES KAPITAL FÜR EUROPÄISCHE SCHLÜSSELTECHNOLOGIEN MOBILISIEREN

Digitale Souveränität erfordert neben leistungsfähigen Technologien und Unternehmen auch ausreichend Kapital für deren Entwicklung und internationale Skalierung. In Europa fehlt es gerade bei strategisch relevanten digitalen Technologien häufig an ausreichend großem und langfristig verfügbarem Kapital für die Wachstumsphase vielversprechender Unternehmen.

Gleichzeitig investieren europäische institutionelle Anleger erhebliche Summen in globale Technologieunternehmen. Das ist aus Sicht von Diversifikation und Rendite grundsätzlich nachvollziehbar, wird aber problematisch, wenn Europa einerseits große Teile seines Kapitals in bereits marktbeherrschende außereuropäische Technologieunternehmen investiert, andererseits aber zu wenig Kapital für den Aufbau eigener technologischer Fähigkeiten mobilisiert. Ziel sollte daher sein, mehr attraktive europäische Investitionsmöglichkeiten zu schaffen und öffentliches Kapital gezielt als strategischen Hebel einzusetzen.¹²³

Wir schlagen deshalb folgende Maßnahmen vor:

- **Strategische Investitionsmandate für öffentliche Fonds:** Staatlich kontrollierte Investitions- und Beteiligungsfonds sollten digitale Souveränität stärker als Ziel berücksichtigen. Im Mittelpunkt sollten europäische Unternehmen in strategisch relevanten Bereichen wie Cloud, Halbleiter, KI, Cybersecurity, digitale Infrastruktur, Datenplattformen und Open-Source-basierte Geschäftsmodelle stehen. Öffentliche Instrumente sollten insbesondere auf Scale-ups und kapitalintensive Schlüsseltechnologien ausgerichtet werden und staatliche und europäische Fonds gezielt als Ankerinvestoren auftreten, um zusätzliches privates Kapital zu mobilisieren.¹²⁴
- **Strategische Technologien langfristig finanzieren:** Investitionen in digitale Souveränität benötigen häufig einen längeren Zeithorizont als klassische Venture-Capital-Modelle. Öffentliche Investoren sollten deshalb stärker sogenanntes Patient Capital bereitstellen und langfristige technologische Entwicklung ermöglichen.¹²⁵
- **Marktmacht eigener Anteilseigner berücksichtigen:** Institutionelle Investoren und Aufsichtsbehörden sollten hohe Konzentrationen in wenigen globalen Technologieunternehmen sowie daraus entstehende Markt-, geopolitische und regulatorische Risiken angemessen in ihrem Risikomanagement berücksichtigen.
- **Anreize schaffen:** Der Staat sollte insbesondere über attraktive Investitionsmöglichkeiten, geeignete Fondsstrukturen und Risikoteilung Anreize für Investitionen in europäische Schlüsseltechnologien schaffen.
- **Kapitalmärkte stärken und vernetzte Förderung:** Europa muss seine Kapitalmärkte vertiefen und integrieren, um ausreichend große Finanzierungsrunden für technologische Schlüsselindustrien zu ermöglichen. Entscheidend ist die stärkere Verzahnung nationaler und EU-weiter Instrumente sowie die Kombination von öffentlicher Forschungsförderung, Transferprogrammen, strategischer Beschaffung und privatem Beteiligungskapital. So lässt sich vermeiden, dass vielversprechende Technologien trotz erfolgreicher Grundlagenforschung oder Start-up-Phase am fehlenden Wachstumskapital scheitern.¹²⁶

Digitale Souveränität benötigt nicht nur technologische, sondern auch finanzielle Handlungsfähigkeit. Europa sollte deshalb einen größeren Teil seines öffentlichen und privaten Kapitals dafür mobilisieren, wettbewerbsfähige eigene Technologieunternehmen und Infrastrukturen aufzubauen.



BILDUNG & GESELLSCHAFT

Digitale Souveränität entsteht nicht allein durch Technologie, Regulierung oder wirtschaftliche Alternativen. Sie setzt auch **Menschen** voraus, **die digitale Systeme verstehen, kritisch beurteilen und selbstbestimmt nutzen können**. In einer Gesellschaft, die immer stärker von digitalen Technologien geprägt wird, entscheidet digitale Souveränität darüber, wie selbstbestimmt Menschen am sozialen, wirtschaftlichen und politischen Leben teilnehmen können. Sie müssen die Möglichkeit bekommen, diese Technologien kompetent, kritisch und verantwortungsvoll zu nutzen. Insbesondere Bildungseinrichtungen tragen eine Verantwortung, diese Kompetenzen zu vermitteln und Alternativen aufzuzeigen.

Gleichzeitig darf digitale Souveränität nicht allein zur Verantwortung des Einzelnen erklärt werden. Individuelle Kompetenz kann fehlende Transparenz, marktbeherrschende Strukturen oder mangelnde Wahlmöglichkeiten nicht ausgleichen. **Staat, Wirtschaft, Bildungseinrichtungen und Technologieanbieter müssen deshalb Rahmenbedingungen schaffen**, die Teilhabe, Barrierefreiheit, Transparenz und echte Wahlmöglichkeiten ermöglichen.

Digitale Souveränität ist damit sowohl eine **Bildungs- als auch eine gesellschaftspolitische Aufgabe**. Eine souveräne digitale Gesellschaft braucht Menschen, die digitale Technologien kompetent und kritisch nutzen können – und Strukturen, die ihnen ermöglichen, diese Entscheidungen tatsächlich selbstbestimmt zu treffen.^{127, 128}

BILDUNG & GESELLSCHAFT

- 1 Bildungseinrichtungen auf souveräne digitale Infrastrukturen umstellen
- 2 Digitale Souveränitätskompetenz stärken
- 3 Digitale Mündigkeit und selbstbestimmte Teilhabe ermöglichen
- 4 Vereine, Organisationen und Parteien als Vorreiter
- 5 Regionale und sektorübergreifende Vernetzung
- 6 Recht auf digitale Selbstbestimmung

1 BILDUNGSEINRICHTUNGEN AUF SOUVERÄNE DIGITALE INFRASTRUKTUREN UMSTELLEN

Digitale Souveränität sollte bereits in Bildungseinrichtungen verankert werden. (Hoch-)Schulen und andere Bildungseinrichtungen prägen den Umgang mit digitalen Technologien und bilden zugleich auch die Grundlage für die digitale Kompetenz künftiger Generationen. Werden dort frühzeitig offene und souveräne Lösungen eingesetzt, können Abhängigkeiten von einzelnen Anbietern reduziert und digitale Selbstbestimmung praktisch vermittelt werden.

“

Wir haben über eine Generation hinaus Menschen an Microsoft-Produkten geschult. [...] Die kamen dann ins Berufsleben rein und haben im Microsoft-Monopol dort weiter in der Wirtschaft arbeiten können.

Mittlerweile wird uns aber bewusst, dass wir uns abhängig gemacht haben von wenigen Unternehmen, die die digitalen Infrastrukturen kontrollieren [...] und die auch jedes Jahr mit Lizenzgebühren immer mehr Geld aus dem Bildungssystem ziehen.¹²⁹

”

Markus Beckedahl

Ziel muss deshalb eine schrittweise Transformation hin zu digitalen Infrastrukturen sein, die Datenkontrolle, offene Standards, Wechselmöglichkeiten und langfristige Handlungsfähigkeit gewährleisten. Open-Source-Lösungen spielen dabei eine besonders wichtige Rolle, weil sie Transparenz, Anpassbarkeit und herstellerunabhängigen Betrieb ermöglichen können.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Souveränitätsstrategie für Bildungs-IT:** Bundesländer, Schulträger und Hochschulen müssen verbindliche Transformationsstrategien für ihre digitale Infrastruktur entwickeln. Bestehende Systeme und Abhängigkeiten müssen zunächst systematisch erfasst und nach Kritikalität bewertet werden. Dazu braucht es klare Übergangsfristen, Migrationspläne und technische Unterstützung – gerade bei der Übertragung bestehender Daten und Systemintegration.¹³⁰
- **Souveräne Lösungen als Ziel:** Bund und Länder sollten die Umstellung von Bildungseinrichtungen auf souveräne IT-Infrastrukturen und Open-Source-Lösungen verbindlich als Ziel im Bildungswesen verankern. Bei neuen IT-Systemen und Softwarelösungen sind offene Standards, Interoperabilität, Auditierbarkeit und Exit-Fähigkeit sicherzustellen. Schnittstellen und Exportmöglichkeiten müssen einen späteren Anbieterwechsel ermöglichen.^{131, 132}

- **Open Source bevorzugt einsetzen:** Wo funktional geeignete, sichere und nachhaltig betreibbare Open-Source-Lösungen verfügbar sind, sollten sie bei Beschaffungsentscheidungen bevorzugt berücksichtigt werden. Insbesondere bei Standardanwendungen, Kollaborationen, Kommunikation, Lernplattformen und digitalen Basisdiensten.
- **Zentrale souveräne Dienste bereitstellen:** Schulen beim Aufbau und Betrieb souveräner IT-Infrastrukturen unterstützt werden. Länder, Kommunen und Hochschulverbünde sollten gemeinsame Dienste z. B. für Identitätsmanagement, Dateiablage, Lernplattformen, Kommunikation und sichere Backups bereitstellen.¹³³
- **Fortbildungen:** Lehrkräfte und pädagogisches Personal müssen mit praxisnahen Fortbildungen an die neuen Lösungen herangeführt werden. Ihre Anforderungen und Praxiserfahrung müssen bei der Einführung sowie bereits bei der Auswahl in die Entscheidung mit einfließen, um Unsicherheiten abzubauen und die Alternativen als Chance wahrzunehmen.¹³⁴

Mit der Umstellung auf souveräne digitale Lösungen wird nicht nur eine langfristig unabhängige Bildungsstruktur geschaffen, sondern auch ein souveräner Umgang mit digitalen Technologien geprägt, den Schülerinnen und Schüler in die Arbeitswelt und Gesellschaft tragen. **Bildung sollte nicht an einzelne Produkte gewöhnen, sondern den souveränen Umgang mit digitalen Werkzeugen vermitteln.**¹³⁵

2 DIGITALE SOUVERÄNITÄTSKOMPETENZ STÄRKEN

Digitale Kompetenzen müssen in Schulen und anderen Bildungseinrichtungen stärker gefördert werden. Digitale Bildung darf sich dabei nicht auf die Bedienung einzelner Produkte beschränken. Menschen müssen grundlegende digitale Konzepte verstehen, unterschiedliche technologische Modelle kennenlernen und anhand nachvollziehbarer Kriterien selbst entscheiden können, welche Technologien sie nutzen möchten.

Bildungseinrichtungen prägen frühzeitig, welche digitalen Werkzeuge und Ökosysteme als selbstverständlich wahrgenommen werden. Wer nur mit einzelnen proprietären Plattformen oder Anwendungen arbeitet, greift auch später eher darauf zurück. Daher ist es entscheidend, nicht bloß die Anwendung souveräner Lösungen zu erlernen, sondern auch ihre Notwendigkeit zu verstehen.¹³⁶

Wir schlagen deshalb folgende Maßnahmen vor:

- **Produktunabhängige Digitalkompetenz vermitteln:** Bildungsangebote sollten grundlegende Konzepte vermitteln, statt sich auf die Bedienung einzelner Marken oder Produkte zu konzentrieren.
- **Alternativen praktisch erfahrbar machen:** Lernende sollten unterschiedliche proprietäre und offene Anwendungen tatsächlich nutzen und vergleichen können. Dazu gehören insbesondere Open-Source-Lösungen, offene Standards und alternative Plattformmodelle. Dafür müssen ihre Wahl- und Bewertungskompetenzen im Hinblick auf Kriterien wie z. B. Datenschutz, offene Standards und Exit-Fähigkeit gefördert werden. Diese Aspekte müssen fest in den Curricula verankert werden.
- **Digitale Markt- und Machtstrukturen verstehen:** Bildung sollte vermitteln, wie Netzwerkeffekte, Plattformmärkte, Datenkonzentration und Vendor Lock-in entstehen und welche wirtschaftlichen und gesellschaftlichen Folgen daraus entstehen können.^{137, 138}
- **Informations- und Medienkompetenz stärken:** Lernende müssen Quellen bewerten, manipulative oder synthetische Inhalte einordnen und verstehen können, wie algorithmische Empfehlungssysteme Sichtbarkeit und öffentliche Kommunikation beeinflussen. Dazu gehört auch, die Funktionsweise, Fähigkeiten und Grenzen von KI-Systemen einschätzen zu können.¹³⁹
- **Bildungspersonal qualifizieren:** Damit digitale Souveränitätskompetenz vermittelt werden kann, benötigen Lehrkräfte und andere Multiplikatorinnen und Multiplikatoren geeignete Fortbildungen und ausreichend Unterstützung für die Auseinandersetzung mit neuen Technologien.¹⁴⁰
- **Lebenslanges Lernen:** Auch Hochschulen, berufliche Weiterbildung etc. müssen Menschen dabei unterstützen, mit neuen Technologien und sich verändernden digitalen Abhängigkeiten kompetent umzugehen.

Digitale Kompetenz bedeutet nicht nur, digitale Anwendungen möglichst effizient bedienen zu können. Eine souveräne digitale Gesellschaft braucht Menschen, die Technologien verstehen, Alternativen kennen, Chancen und Risiken abwägen und selbstbestimmt entscheiden können, welche digitalen Werkzeuge sie nutzen wollen.

3 DIGITALE MÜNDIGKEIT UND SELBSTBESTIMMTE TEILHABE ERMÖGLICHEN

Digitale Souveränität setzt Menschen voraus, die digitale Technologien nicht nur kompetent nutzen, sondern ihre Entscheidungen auch bewusst und eigenverantwortlich treffen können. Digitale Mündigkeit bedeutet, Chancen, Risiken und Abhängigkeiten digitaler Angebote einschätzen, eigene Interessen vertreten und vorhandene Wahlmöglichkeiten selbstbestimmt nutzen zu können.

Diese Verantwortung darf jedoch nicht auf den Einzelnen abgeschoben werden. Menschen können nur dann souverän entscheiden, wenn tatsächlich Alternativen existieren, Informationen verständlich verfügbar sind und gesellschaftliche Teilhabe nicht unnötig an einzelne Plattformen, Anbieter oder Technologien gebunden wird. Staat, Bildungseinrichtungen, Wirtschaft und Technologieanbieter tragen deshalb eine besondere Verantwortung dafür, solche Rahmenbedingungen zu schaffen.^{141, 142}

Wir schlagen deshalb folgende Maßnahmen vor:

- **Eigenverantwortliche Entscheidungen ermöglichen:** Menschen sollten darin unterstützt werden, die Konsequenzen ihrer digitalen Entscheidungen zu reflektieren – beispielsweise hinsichtlich Datenschutz, Sicherheit, Plattformwahl, KI-Nutzung oder der Weitergabe persönlicher Informationen.
- **Wahlfreiheit und offene Teilhabe sichern:** Digitale Mündigkeit setzt voraus, dass Menschen zwischen verschiedenen digitalen Angeboten wählen können und gesellschaftliche Teilhabe nicht an die Nutzung bestimmter kommerzieller Plattformen oder proprietärer Anwendungen geknüpft ist. Wo öffentliche oder gesellschaftlich notwendige Leistungen betroffen sind, müssen angemessene alternative Zugangswege erhalten bleiben.¹⁴³
- **Minimierung des Digitalzwangs:** Digitale Angebote sollen den Zugang zu öffentlichen und gesellschaftlich relevanten Leistungen erleichtern, nicht zur Voraussetzung machen. Wo ein Ausschluss durch fehlenden digitalen Zugang droht, müssen analoge und persönliche Zugangswege erhalten bleiben. Das gilt insbesondere für Verwaltung, Bildung und soziale Leistungen.¹⁴⁴
- **Zivilgesellschaftliche Strukturen stärken:** Verbraucherorganisationen, Medienbildung, Open-Source-Communities und andere zivilgesellschaftliche Akteure leisten einen wichtigen Beitrag zur digitalen Mündigkeit. Ihre Informations-, Beratungs- und Beteiligungsangebote sollten langfristig unterstützt werden.¹⁴⁵

Digitale Mündigkeit bedeutet damit weder, jede technologische Entscheidung dem Staat zu überlassen, noch die Verantwortung für strukturelle Probleme vollständig auf den Einzelnen abzuwälzen. Eine souveräne digitale Gesellschaft braucht Menschen, die informiert und eigenverantwortlich handeln können – und Rahmenbedingungen, die ihnen echte Wahlmöglichkeiten, Rechte und gesellschaftliche Teilhabe ermöglichen.

4

VEREINE, ORGANISATIONEN & PARTEIEN ALS VORREITER

Digitale Alternativen können sich nur etablieren, wenn sie tatsächlich genutzt werden. Vereine, Verbände, zivilgesellschaftliche Organisationen und politische Parteien haben eine besondere Vorbildfunktion, denn sie prägen gesellschaftliche Kommunikationsgewohnheiten, schaffen Reichweite und können dazu beitragen, alternative digitale Angebote sichtbar und alltags-tauglich zu machen.¹⁴⁶

Gerade politisch und gesellschaftlich relevante Informationen sollten nicht ausschließlich über einzelne kommerzielle Plattformen zugänglich sein. Wer öffentliche Kommunikation vollständig an wenige proprietäre Plattformen bindet, verstärkt deren Netzwerkeffekte und erschwert es Menschen, sich außerhalb dieser Ökosysteme zu informieren. Gesellschaftliche Organisationen sollten deshalb ihre Kommunikationswege diversifizieren und offene sowie selbst kontrollierbare Kanäle stärken.

Wir schlagen deshalb folgende Maßnahmen vor:

- **+1-Regel auch gesellschaftlich anwenden:** Vereine, Verbände, Organisationen und Parteien sollten zentrale Inhalte nicht ausschließlich auf einzelnen kommerziellen Plattformen veröffentlichen, sondern mindestens einen zusätzlichen offenen oder selbst kontrollierten Kommunikationskanal anbieten.¹⁴⁷ Vor allem politische Parteien, die die demokratische Öffentlichkeit vorrangig mitgestalten, sind hier in einer besonderen Verantwortung.
- **Alternative und offene Plattformen nutzen:** Organisationen sollten gezielt auch föderierte, interoperable oder anderweitig offene Plattformen nutzen und damit deren Sichtbarkeit und Reichweite erhöhen. Das Argument, alternative Plattformen seien aufgrund geringer Nutzerzahlen nicht relevant, darf nicht dazu führen, dass notwendige Netzwerkeffekte niemals entstehen können.¹⁴⁸
- **Eigene digitale Präsenz als Basis stärken:** Websites, Newsletter und andere selbst kontrollierbare Angebote sollten den dauerhaften Kern der digitalen Kommunikation bilden. So bleiben Informationen unabhängig von den Algorithmen oder Entscheidungen einzelner Plattformanbieter zugänglich.^{149, 150}
- **Eigene IT-Nutzung überprüfen:** Die Vorbildfunktion gesellschaftlicher Organisationen beschränkt sich nicht auf soziale Medien. Auch bei Kommunikationsdiensten, Cloud-Speichern, Dokumentenformaten und KI-Anwendungen sollte die Verringerung unnötiger technologischer Abhängigkeiten geprüft werden.¹⁵¹
- **Erfahrungen sichtbar machen:** Erfolgreiche Migrationen und alternative Kommunikationsstrategien sollten dokumentiert und öffentlich geteilt werden. Praxisbeispiele können anderen Organisationen zeigen, was funktioniert und welche Herausforderungen bei einem Wechsel entstehen.

Gesellschaftliche Organisationen können digitale Souveränität nicht nur fordern, sondern durch eigenes Handeln konkret unterstützen. Gerade Organisationen mit gesellschaftlicher und politischer Reichweite können dazu beitragen, dass neue Netzwerkeffekte entstehen und digitale Kommunikation weniger abhängig von einzelnen privatwirtschaftlichen Plattformen wird.

5

REGIONALE UND SEKTORÜBERGREIFENDE VERNETZUNG

Digitale Souveränität lässt sich weder von einzelnen Unternehmen noch von Politik, Wissenschaft oder Zivilgesellschaft allein herstellen. Viele technologische Abhängigkeiten betreffen mehrere gesellschaftliche und wirtschaftliche Bereiche gleichzeitig. Umso wichtiger ist es, Wissen, Bedarfe und Ressourcen stärker zu bündeln und gemeinsame Lösungen zu entwickeln.

Gerade Akteure aus Wirtschaft, Medien, Wissenschaft, Bildung, Verbraucherschutz, Zivilgesellschaft und öffentlicher Hand können sich dabei sinnvoll ergänzen. Durch den Austausch von Wissen, Erfahrungen und Ressourcen können gemeinsame Lösungen entwickelt und bestehende Abhängigkeiten verringert werden. Vernetzte Akteure sind zudem besser in der Lage, ihre Interessen gegenüber Politik und Wirtschaft zu vertreten und alternative digitale Angebote aufzubauen.

Wir schlagen deshalb folgende Maßnahmen vor:

- **Sektorübergreifende Netzwerke stärken:** Es braucht eine stärkere Vernetzung oben genannter Akteure, um technologische Abhängigkeiten gemeinsam zu analysieren und Lösungen zu entwickeln. Dabei können erfolgreiche Migrationen, geeignete Technologien, neue Geschäftsmodelle und praktische Erfahrungen über gemeinsame Plattformen, Workshops und Austauschformate zugänglich gemacht werden.¹⁵²
- **Anbieter und Nachfrager zusammenbringen:** Europäische Technologieanbieter, Open-Source-Projekte und Anwenderorganisationen müssen leichter zueinanderfinden. Matchmaking, Demonstratoren und gemeinsame Pilotprojekte können dazu beitragen, vorhandene Lösungen schneller in die Anwendung zu bringen und neue Anforderungen frühzeitig an Anbieter zurückzuspielen.
- **Gemeinsame Nachfrage organisieren:** Wo mehrere Organisationen ähnliche Anforderungen haben, sollten gemeinsame Beschaffungsmodelle, Rahmenverträge oder abgestimmte Ausschreibungen geprüft werden. Gebündelte Nachfrage kann insbesondere kleineren europäischen Anbietern helfen, Skalierung und Marktzugang zu erreichen. Gemeinsam könnten auch Förder- und Innovationsprojekte initiiert werden, um neue Lösungen zu entwickeln und zu prüfen.¹⁵³
- **Regionale Reallabore ermöglichen:** Regionen mit einer starken Verbindung von Wirtschaft, Forschung und gesellschaftlichen Akteuren sollten neue souveräne Technologien und Kooperationsmodelle praktisch erproben können. Erfolgreiche Ansätze können anschließend auf andere Regionen und Branchen übertragen werden.
- **Dauerhafte Strukturen schaffen:** Fördermittel können den Aufbau von Netzwerken und erste Pilotprojekte unterstützen. Langfristig sollten jedoch tragfähige Organisations- und Geschäftsmodelle entstehen, damit Kooperationen nicht mit dem Ende einzelner Förderprojekte verschwinden.

OWL als regionale Pilotregion

Für Ostwestfalen-Lippe planen die herausgebenden Organisationen gemeinsam mit InnoZent OWL den Aufbau eines regionalen Austauschnetzwerks für digitale Souveränität. Das Netzwerk soll Unternehmen und weitere Akteure auf dem Weg zu mehr digitaler Souveränität begleiten und insbesondere Anbieter und Nachfrager souveräner Technologien zusammenbringen.

Über den reinen Erfahrungsaustausch hinaus soll daraus ein regionales Innovations- und Transferökosystem entstehen. Gemeinsame Bedarfe können identifiziert, Technologien praktisch erprobt und neue Kooperations- oder Förderprojekte initiiert werden. Perspektivisch können daraus auch Impulse für gemeinsame digitale Infrastrukturen entstehen, beispielsweise für regionale Rechenzentrums- und Cloud-Angebote, Datenräume, KI-Infrastrukturen oder gemeinsame Cybersecurity-Dienste.

OWL kann damit als regionale Pilotregion zeigen, wie digitale Souveränität durch das Zusammenspiel von Wirtschaft, Wissenschaft, Technologieanbietern, öffentlicher Hand und Zivilgesellschaft praktisch vorangebracht werden kann. Erfolgreiche Ansätze können anschließend als Vorbild für andere Regionen dienen.

Digitale Souveränität braucht funktionierende Ökosysteme, in denen Akteure ihre Kompetenzen, Bedarfe und Ressourcen verbinden. Regionale und sektorübergreifende Netzwerke können dazu beitragen, aus einzelnen Alternativen tragfähige Märkte, Infrastrukturen und gemeinsame Handlungsfähigkeit entstehen zu lassen.



RECHT AUF DIGITALE SELBSTBESTIMMUNG

Jeder und jede hat das Recht auf digitale Selbstbestimmung – darf also selbst über das entscheiden, was er oder sie preisgibt und wie diese Daten verwendet werden. Das Recht auf informationelle Selbstbestimmung bildet seit den 1980er-Jahren eine zentrale Grundlage des Datenschutzes in Deutschland.¹⁵⁴

Sein Grundgedanke bleibt hochaktuell: Menschen müssen grundsätzlich darüber bestimmen können, welche personenbezogenen Informationen über sie erhoben und wie diese verwendet werden. Die digitale Welt hat sich jedoch erheblich weiterentwickelt. Profiling, Künstliche Intelligenz und automatisierte Entscheidungssysteme ermöglichen es heute, nicht nur vorhandene Informationen zu verarbeiten, sondern aus großen Datenmengen neue Eigenschaften, Wahrscheinlichkeiten und Prognosen über einzelne Menschen oder Gruppen abzuleiten.

Digitale Selbstbestimmung muss deshalb über die bewusste Preisgabe persönlicher Daten hinausgedacht werden. Entscheidend ist nicht nur, welche Informationen eine Person selbst zur Verfügung stellt, sondern auch, welche Aussagen über sie algorithmisch erzeugt werden, wie diese verwendet werden und welche Folgen daraus entstehen. Solche Zuschreibungen können Menschen beeinflussen, selbst wenn sie unvollständig oder falsch sind.

Gleichzeitig setzt Selbstbestimmung echte Wahlmöglichkeiten voraus. Eine formale Zustimmung zu Datenverarbeitung reicht nicht aus, wenn die Ablehnung mit erheblichen Nachteilen verbunden ist oder ein Dienst faktisch alternativlos geworden ist. Digitale Selbstbestimmung benötigt deshalb sowohl individuelle Rechte als auch technische und wirtschaftliche Rahmenbedingungen, die tatsächliche Wahlfreiheit ermöglichen.

„Mit dem Begriff der prädiktiven Privatheit findet somit eine Bereichserweiterung statt: In die Domäne ihrer informationellen Selbstbestimmung fallen nicht nur Informationen, die Sie kontrollieren können, sondern auch solche, die über Sie geschätzt werden, unabhängig vom Wahrheitsgehalt der Schätzung. Das so zu sehen, ist keine Selbstverständlichkeit, denn den meisten Menschen ist aktuell nicht klar, dass digitale Geschäftsmodelle heute systematisch auf der Verwendung abgeleiteter Informationen über (ggf. sogar anonyme) Datensubjekte beruhen.“¹⁵⁵

Wir schlagen deshalb folgende Maßnahmen vor:

- **Informationelle Selbstbestimmung für die digitale Welt weiterentwickeln:** Bestehende Datenschutz- und Persönlichkeitsrechte müssen so konkretisiert und durchgesetzt werden, dass sie den Herausforderungen durch Profiling, KI, automatisierte Entscheidungen und datengetriebene Geschäftsmodelle gerecht werden. Dabei darf der Schutz persönlicher Informationen nicht dort enden, wo Menschen Daten bewusst preisgegeben haben.¹⁵⁶ Er muss auch sensible Eigenschaften, Kategorien und Prognosen erfassen, die aus vorhandenen Daten über Personen oder Gruppen abgeleitet werden.

- **Folgenreiche Profilbildung transparent machen:** Menschen müssen nachvollziehen können, wenn über sie automatisiert Profile, Bewertungen oder Prognosen erstellt werden, die wesentliche Auswirkungen auf ihre Chancen, Sichtbarkeit oder Behandlung haben können. Dazu gehört auch Transparenz darüber, welche Daten und wesentlichen Kriterien in solche Bewertungen einfließen.¹⁵⁷
- **Recht auf Anfechtung:** Betroffene müssen algorithmische Bewertungen und automatisierte Entscheidungen nachvollziehen und anfechten, fehlerhafte Ergebnisse korrigieren lassen und eine menschliche Überprüfung verlangen können.¹⁵⁸
- **Echte Einwilligung:** Zustimmung zur Datenverarbeitung muss freiwillig erfolgen. Daten, die für die Erbringung eines Dienstes nicht erforderlich sind, dürfen nicht allein deshalb zur Voraussetzung gemacht werden, weil Nutzende andernfalls faktisch vom Zugang zu einem relevanten Angebot ausgeschlossen wären.¹⁵⁹
- **Digitale Identität schützen:** Digitale Selbstbestimmung umfasst auch die Kontrolle über die eigene digitale Darstellung. Bild, Stimme und andere identitätsprägende Merkmale müssen vor missbräuchlicher synthetischer Erzeugung, Manipulation oder Verwendung geschützt werden.¹⁶⁰
- **Datensparsamkeit und Privacy by Design:** Digitale Dienste müssen so gestaltet werden, dass möglichst wenige personenbezogene Daten erforderlich sind und datenschutzfreundliche Einstellungen standardmäßig gewählt werden. Selbstbestimmung darf nicht davon abhängen, dass Nutzende komplexe Einstellungen eigenständig korrigieren müssen.
- **Wirksame Rechtsdurchsetzung:** Rechte entfalten nur dann Wirkung, wenn Menschen sie tatsächlich wahrnehmen können. Beschwerdewege, Auskunftsrechte, Korrekturmöglichkeiten und Aufsichtsstrukturen müssen deshalb verständlich, niedrigschwellig und effektiv ausgestaltet sein.¹⁶¹

Digitale Selbstbestimmung bedeutet heute mehr als die Kontrolle darüber, welche Informationen Menschen selbst preisgeben. In einer zunehmend datengetriebenen Gesellschaft stellt sich ebenso die Frage, wer welche Aussagen über Menschen berechnen, daraus Entscheidungen ableiten und diese Entscheidungen praktisch wirksam werden lassen darf. **Eine souveräne digitale Gesellschaft muss sowohl die Kontrolle über persönliche Daten als auch Transparenz, Wahlfreiheit und Schutz gegenüber folgenreicher algorithmischer Profilbildung gewährleisten.**

UNSERE REIHE ZUR DIGITALEN SOUVERÄNITÄT



Vortrag Prof. Martin Andree – 11.02.2026

Der Medienwissenschaftler und Digital-Experte war bei uns in Paderborn zu Gast und sprach vor über 200 Gästen über die größten Gefahren für unsere Demokratie.

Podiumsdiskussion – 20.04.2026

In unserer Podiumsdiskussion haben wir mit Expertinnen und Experten aus Politik, Wirtschaft und Medien diskutiert, wie Europa seine digitale Abhängigkeit von den großen US-amerikanischen Tech-Konzernen zum Schutz unserer Wirtschaft und Demokratie verringern kann und sollte.



Digitaler Workshop zur Diskussion Maßnahmenkatalog – 27.05.2026

Was braucht es, um digitale Souveränität konkret zu erreichen? Gemeinsam haben wir Maßnahmen erarbeitet, die es aus unserer Sicht für dieses Ziel braucht.

Workshop – 23.06.2026

In einem dreistündigen Workshop führte Leena Simon von Digitalcourage durch zehn Schritte zur digitalen Mündigkeit, die zu mehr Selbstbestimmtheit im digitalen Alltag verhelfen sollen.





QUELLEN

Alternativen stärken

- 1: Europäische Union, 14. September 2022, Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreithbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022R1925-20221012>, letzter Zugriff am 05.10.2026
- 2: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main, S. 256
- 3: Europäische Union, 14. September 2022, Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreithbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022R1925-20221012>, letzter Zugriff am 27.08.2026
- 4: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main, S. 256 f.
- 5: Europäische Union, 2026, Messaging Interoperability, https://digital-markets-act.ec.europa.eu/developer-portal/messaging-interoperability_en, letzter Zugriff am 27.08.2026
- 6: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, European Data Protection Board, 20. Oktober 2020, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en, letzter Zugriff am 08.10.2026
- 7: Bundesministerium für Digitales und Staatsmodernisierung, 2026, Digitale Souveränität, <https://bmds.bund.de/themen/digitale-souveraenitaet>, letzter Zugriff am 27.08.2026
- 8: European Data Protection Board, 2026, EDSA bringt Klarheit in die Datenverarbeitung für die wissenschaftliche Forschung, beschleunigt die Fertigstellung der Anonymisierungsleitlinien und genehmigt erstes europäisches Datenschutzsiegel als Instrument für Übermittlungen, https://www.edpb.europa.eu/news/edpb-brings-clarity-to-data-processing-for-scientific-research-speeds-up-the-finalisation-of_de, letzter Zugriff am 27.08.2026
- 9: Schweizerische Eidgenossenschaft, 2026, Datenschutz in der Forschung, <https://www.edoeb.admin.ch/de/datenschutz-in-der-forschung>, letzter Zugriff am 27.08.2026
- 10: Fraunhofer IMS, 2026, Föderiertes Lernen für ressourcenbegrenzte Systeme, <https://www.ims.fraunhofer.de/de/Geschaeftsfeld/Industry/Industrial-AI/Foederiertes-lernen.html>, letzter Zugriff am 27.08.2026
- 11: Lindell, Yehuda, 2020, Secure Multiparty Computation (MPC), <https://eprint.iacr.org/2020/300>, letzter Zugriff am 27.08.2026, DOI: [10.1145/3387108](https://doi.org/10.1145/3387108)

- 12: Zhang et al., 2021, PrivSyn: Differentially Private Data Synthesis, https://publications.cispa.de/articles/conference_contribution/PrivSyn_Differentially_Private_Data_Synthesis/24613539?file=43247859 , letzter Zugriff am 27.08.2026
- 13: Bundesministerium für Forschung, Technologie und Raumfahrt, 2021, Förderung von Datentreuhandmodellen, https://www.bildung-forschung.digital/digitalezukunft/de/wissenschaft_und_forschung/datentreuhandmodelle/datentreuhandmodelle/datentreuhandmodelle_node.html, letzter Zugriff am 27.08.2026
- 14: Massachusetts Institute of Technology (MIT), 2026, Enabling privacy-preserving AI training on everyday devices, <https://news.mit.edu/2026/enabling-privacy-preserving-ai-training-everyday-devices-0429>, letzter Zugriff am 27.08.2026
- 15: CISPA Helmholtz Center for Information Security, 2026, Secure & Privacy Preserving Machine Learning, <https://cispa.de/en/research/research-areas/trustworthy-information-processing/secure-and-privacy-preserving-machine-learning>, letzter Zugriff am 27.08.2026
- 16: Bundesministerium für Digitales und Staatsmodernisierung, 2026, Digitale Souveränität, <https://bmds.bund.de/themen/digitale-souveraenitaet>, letzter Zugriff am 27.08.2026
- 17: Save Social, 2026, Soziale Netzwerke als demokratische Kraft retten, <https://savesocial.eu/de/>, letzter Zugriff am 27.08.2026
- 18: Rockley, Ann & Cooper, Charles; 16. Februar 2012. Managing Enterprise Content: A Unified Content Strategy. New Riders, 2. Auflage
- 19: Singh, Aditya & Warso, Zuzanna; 26. März 2026, public procurement as a strategic lever for digital sovereignty – Open Future Policy Brief, https://openfuture.eu/wp-content/uploads/2026/03/260326_Public-Procurement-as-a-Strategic-Lever-for-Digital-Sovereignty.pdf, letzter Zugriff am 28.08.2026
- 20: Deutscher Bundestag, Wissenschaftliche Dienste, Fachbereich WD 7, 2026, Vergabeverfahren zur Bereitstellung, Entwicklung und Änderung von Computersoftware Zur Zulässigkeit der Beschränkung eines öffentlichen Auftragsgegenstandes auf „Open Source Software“, <https://www.bundestag.de/resource/blob/1165534/WD-7-010-26.pdf>, letzter Zugriff am 28.08.2026
- 21: Europäische Kommission, 2026, The EU Open Source Strategy, <https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>, letzter Zugriff am 28.08.2026
- 22: Europäische Kommission, 19. Mai 2025, How the DIGITAL Building Blocks can help bring EuroStacks vision of European digital sovereignty to life, <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/900014236/How+the+DIGITAL+Building+Blocks+can+help+bring+EuroStacks+vision+of+European+digital+sovereignty+to+life>, letzter Zugriff am 28.08.2026

23: European Digital SME Alliance, 5. Dezember 2025, Tech Sovereignty into action: Digital SME summit unveils Europe´s homegrown digital solutions, <https://www.digitalsme.eu/tech-sovereignty-into-action-digital-sme-summit-unveils-europes-homegrown-digital-solutions/>, letzter Zugriff am 05.10.2026

24: Europäische Kommission, 2026, Interoperable Europe Portal, <https://interoperable-europe.ec.europa.eu/>, letzter Zugriff am 28.08.2026

25: Singh, Aditya & Warso, Zuzanna; 26. März 2026, public procurement as a strategic lever for digital sovereignty – Open Future Policy Brief, https://openfuture.eu/wp-content/uploads/2026/03/260326_Public-Procurement-as-a-Strategic-Lever-for-Digital-Sovereignty.pdf, letzter Zugriff am 28.08.2026

26: Föderale IT-Kooperation (FITKO), Januar 2021, Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf, letzter Zugriff am 05.10.2026

27: Europäische Kommission, 2026, Interoperable Europe Portal, <https://interoperable-europe.ec.europa.eu/>, letzter Zugriff am 28.08.2026

Gesetzliche Regulierung

28: Andree, Martin & Thompsen, Timo, 2020, Atlas der digitalen Welt, Campus Verlag GmbH, Frankfurt am Main

29: Andree, Martin & Peifer, Karl-Nikolaus, April 2023, Digitaler Neustart für freien Wettbewerb und Vielfalt in digitalen Märkten, Medien Wirtschaft, <https://kriegdermedien.de/digitaler-neustart.pdf>, letzter Zugriff am 01.09.2026

30: European Digital Rights (EDRI), 05.02.2025, Why Ireland is the Achilles heel of the EU's fightback against Big Tech, <https://edri.org/our-work/why-ireland-is-the-achilles-heel-of-the-eus-fightback-against-big-tech/>, letzter Zugriff am 01.09.2026

31: Europäische Kommission, 2026, About the Digital Markets Act, https://digital-markets-act.ec.europa.eu/about-dma_en, letzter Zugriff am 02.09.2026

32: Europäische Kommission, 2026, Gesetz über digitale Dienste: Fragen und Antworten, <https://digital-strategy.ec.europa.eu/de/faqs/digital-services-act-questions-and-answers>, letzter Zugriff am 02.09.2026

33: Europäische Kommission, 2026, Digital Services Act (DSA) EU-Regeln für digitale Plattformen - Schutz der Meinungsfreiheit und von Wahlen, https://germany.representation.ec.europa.eu/digital-services-act-dsa-eu-regeln-fur-digitale-plattformen-schutz-der-meinungsfreiheit-und-von_de, letzter Zugriff am 02.09.2026

34: Center For Strategic & International Studies, 13.09.2021, 3 Years Later: An Analysis of GDPR Enforcement, <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement>, letzter Zugriff am 01.09.2026

35: Mattioli, Pietro (Utrecht University), 01.09.2025, Navigating the Complexities of the DSA's Enforcement Framework: Sincere Cooperation in Action?, <https://utrechtlawreview.org/articles/10.36633/ulr.1074>, letzter Zugriff am 01.09.2026

36: Stiftung Neue Verantwortung, 08.02.2024, The Digital Services Act is in effect – now what?, <https://www.interface-eu.org/publications/digital-services-act-now-what>, letzter Zugriff am 01.09.2026

37: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main

38: die medienanstalten, 01.01.2025, Medienstaatsvertrag (MStV), https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Medienstaatsvertrag_MStV.pdf, letzter Zugriff am 02.09.2026

39: Andree, Martin & Peifer, Karl-Nikolaus, April 2023, Digitaler Neustart für freien Wettbewerb und Vielfalt in digitalen Märkten, Medien Wirtschaft, <https://kriegdermedien.de/digitaler-neustart.pdf>, letzter Zugriff am 01.09.2026

40: Save Social, 2026, Soziale Netzwerke als demokratische Kraft retten, <https://savesocial.eu/de/>, letzter Zugriff am 02.09.2026

41: Andree, Martin & Peifer, Karl-Nikolaus, April 2023, Digitaler Neustart für freien Wettbewerb und Vielfalt in digitalen Märkten, Medien Wirtschaft, <https://kriegdermedien.de/digitaler-neustart.pdf>, letzter Zugriff am 01.09.2026

42: Lewanczik, Niklas (OnlineMarketing.de GmbH), 07.11.2025, Meta verdient Milliarden mit Ads für Scams und Verbotenes, <https://onlinemarketing.de/social-media-marketing/meta-verdient-milliarden-ads-fuer-scams>, letzter Zugriff am 02.09.2026

43: Andree, Martin & Peifer, Karl-Nikolaus, April 2023, Digitaler Neustart für freien Wettbewerb und Vielfalt in digitalen Märkten, Medien Wirtschaft, <https://kriegdermedien.de/digitaler-neustart.pdf>, letzter Zugriff am 01.09.2026

44: Bundesministerium der Justiz und für Verbraucherschutz, 2026, Bürgerliches Gesetzbuch (BGB) § 242 Leistung nach Treu und Glauben, https://www.gesetze-im-internet.de/bgb/_242.html, letzter Zugriff am 03.09.2026

45: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main

46: Save Social, 2026, Soziale Netzwerke als demokratische Kraft retten, <https://savesocial.eu/de/>, letzter Zugriff am 03.09.2026

47: Institut der Deutschen Wirtschaft, 23. Mai 2025, IW-Kurzbericht 47/2025, Digitalsteuern als Gegenmaßnahme im US-Handelsstreit?, <https://www.iwkoeln.de/studien/samina-sultan-digitalsteuern-als-gegenmassnahme-im-us-handelsstreit.html> letzter Zugriff am 03.09.2026

48: Schinkels, Pauline & Von Lindern, Jakob (Zeitverlag Gerd Bucerius GmbH & Co. KG), 10.04.2025, Was eine Digitalsteuer wirklich bringt, <https://www.zeit.de/digital/2025-04/digitalsteuer-eu-us-zoelle-tech-konzerne-faq#was-ist-eine-digitalsteuer>, letzter Zugriff am 03.09.2026

49: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main

50: EuroStack, 2026, Building Europe´s digital future, <https://eurostack.eu/>, letzter Zugriff am 03.09.2026

51: Andree, Martin & Thompson, Timo, 2020, Atlas der digitalen Welt, Campus Verlag GmbH, Frankfurt am Main

52: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main

53: Prof. Dr. Martin Andree, 2023, Big Tech muss weg, Campus Verlag GmbH, Frankfurt am Main

54: Europäische Kommission, 2026, The EU Open Source Strategy, <https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>, letzter Zugriff am 03.09.2026

- 55: Europäische Kommission: Generaldirektion für Wettbewerb, Crémer, J., Montjoye, Y.-A. d. and Schweitzer, H., 2019, Competition policy for the digital era, Publications Office, <https://data.europa.eu/doi/10.2763/407537>, letzter Zugriff am 03.09.2026
- 56: Organisation for Economic Co-operation and Development, 10.06.2020, Start-ups, Killer Acquisitions and Merger Control – Background Note, [https://one.oecd.org/document/DAF/COMP\(2020\)5/en/pdf](https://one.oecd.org/document/DAF/COMP(2020)5/en/pdf), letzter Zugriff am 03.09.2026
- 57: DIE ZEIT online, 27.12.2021, Bundeskartellamt fordert mehr Personal und größeren Etat, <https://www.zeit.de/wirtschaft/2021-12/bundeskartellamt-verbraucher-konzerne-personal-etat-ressourcen>, letzter Zugriff am 03.09.2026
- 58: De la Vega, D., Urheberrecht und KI-Training, IRIS, Europäische Audiovisuelle Informationsstelle, Straßburg, Juli 2026
- 59: Deutscher Kulturrat, 01.03.2021, Vorgehen bei Urheberrechtsverletzungen, <https://www.kulturrat.de/themen/urheberrecht/vorgehen-bei-urheberrechtsverletzungen/>, letzter Zugriff am 03.09.2026
- 60: Europäisches Parlament, 10.03.2026, Schutz von Urheberrecht und kreativer Arbeit im Zeitalter künstlicher Intelligenz, <https://www.europarl.europa.eu/news/de/press-room/20260306IPR37511/schutz-von-urheberrecht-kreativer-arbeit-im-zeitalter-kunstlicher-intelligenz>, letzter Zugriff am 03.09.2026
- 61: Die Bundesregierung, 11.02.2026, AI-Act – Einheitliche Regeln für Künstliche Intelligenz in der EU, <https://www.bundesregierung.de/breg-de/aktuelles/ai-act-2285944>, letzter Zugriff am 03.09.2026
- 62: Europäische Union, 13. Juni 2024, Verordnung (EU) 2024/1689 (AI Act), Art. 50 Abs. 2 und Art. 50 Abs. 4., https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689, letzter Zugriff am 07.10.2026
- 63: Kettemann, Matthias & Schulz, Wolfgang, Alexander von Humboldt Institut für Internet und Gesellschaft, 07.07.2026, Between accusations of censorship and platform power: What the Digital Services Act actually regulates, <https://www.hiig.de/en/between-accusations-of-censorship-and-platform-power/>, letzter Zugriff am 03.09.2026
- 64: Botan, M. (2026). Accountability in name only: Fact-checking under the EU's Code of Practice on Disinformation. Harvard Kennedy School (HKS) Misinformation Review. <https://doi.org/10.37016/mr-2020-203>
- 65: Stürmer, Ariane (Bayrischer Rundfunk), 10.05.2026, Profil blockiert, Content weg: Wie Instagram das entscheidet, <https://www.br.de/nachrichten/netzwelt/profil-blockiert-content-weg-wie-instagram-das-entscheidet,Vlee5cp>, letzter Zugriff am 03.09.2026
- 66: Europäische Union, 12. April 2023, Gesetz über digitale Dienste/Digital Services Act (DSA), Art. 17, <https://eur-lex.europa.eu/legal-content/DE/LSU/?uri=CELEX:32022R2065>, letzter Zugriff am 07.10.2026
- 67: Appeals Centre Europe, 09.04.2025, New EU Network Helps Users to Challenge Online Platforms' Decisions, <https://www.appealscentre.eu/eu-digital-services-act-ods-network-launch/>, letzter Zugriff am 03.09.2026

68: Art. 21 Abs. 3 Buchst. a und c der Verordnung (EU) 2022/2065 (Digital Services Act) sowie Verordnung (EU) 2022/2065 (Digital Services Act), insbesondere Art. 45 Abs. 1 und 2 sowie Art. 34 und 35 unter Berücksichtigung von Erwägungsgrund 90

69: Hong, Eunseo (Courthouse News Service), 27.05.2026, Big Tech's moderation mistakes are piling up in Europe's appeals system, <https://courthousenews.com/big-techs-moderation-mistakes-are-piling-up-in-europes-appeals-system/>, letzter Zugriff am 03.09.2026

70: Art. 20 DSGVO (Datenübertragbarkeit) sowie Art. 18 Abs. 1 lit. c DSGVO i. V. m. Art. 20 Verordnung (EU) 2022/2065 (DSA)

71: Davy, Max, Oxford Internet Institute, 08.01.2026, The Missing Metrics in DSA Content Moderation Transparency, DSA Observatory, <https://dsa-observatory.eu/2026/01/08/the-metrics-were-missing-in-dsa-content-moderation-transparency/>, letzter Zugriff am 03.09.2026

72: UNESCO, *Guidelines for the Governance of Digital Platforms*, 2023, Rn. 35–38 und 89–90

73: ARTICLE 19, 12. Oktober 2021, Social Media Councils: One piece in the puzzle of content moderation, S. 7–8 und 17–18, <https://www.article19.org/resources/social-media-councils-moderation/>, letzter Zugriff am 07.10.2026

74: Europäische Kommission, 2026, Digital Services Act (DSA) EU-Regeln für digitale Plattformen - Schutz der Meinungsfreiheit und von Wahlen, https://germany.representation.ec.europa.eu/digital-services-act-dsa-eu-regeln-fur-digitale-plattformen-schutz-der-meinungsfreiheit-und-von_de, letzter Zugriff am 03.09.2026

Sicherheit

75: Andree, Martin & Thompson, Timo, 2020, Atlas der digitalen Welt, Campus Verlag GmbH, Frankfurt am Main

76: Europäische Kommission, 3. Juni 2026, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy, <https://www.europarl.europa.eu/news/de/agenda/plenary-news/2026-06-15/7/digitale-souveranitat-und-resilienz>, letzter Zugriff am 28.08.2028

77: Open Source Business Alliance, 12. August 2025, 100 Tage Bundesregierung: Wo bleibt die strategische Ausrichtung auf Open Source Software? <https://osb-alliance.de/pressemitteilungen/100-tage-bundesregierung-wo-bleibt-die-strategische-ausrichtung-auf-open-source-software>, letzter Zugriff 28.08.2026

78: Deutsche Industrie- und Handelskammer (DIHK), Juni 2026, Position Digitale und technische Souveränität, <https://www.dihk.de/de/newsroom/dihk-fordert-strategischen-rahmen-fuer-digitale-und-technologische-souveranitaet-182774>, letzter Zugriff am 05.10.2026

79: ZDF-Morgenmagazin, 11.11.2025, Digitale Sicherheit: „Hilflos und kopflos“, Digitale Sicherheit: "Hilflos und kopflos", letzter Zugriff am 28.08.2026

80: Bundesministerium der Finanzen, 15.04.2026, Investitionen der Bundessäule, https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Oeffentliche_Finzen/SVIK/Bund/investitionen-der-bundessauele.html, letzter Zugriff 28.08.2026

81: Bundesministerium der Finanzen, 2026, Haushaltsplan 2026 – Einzelplan 60, <https://www.bundeshaushalt.de/static/daten/2026/soll/epl60.pdf>, letzter Zugriff am 28.08.2026

82: Bundesgesetzblatt, 05.12.2025, Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, <https://www.recht.bund.de/bgbl/1/2025/301/VO.html>, letzter Zugriff am 05.10.2026

83: Lünendonk & Hossenfelder, 30. Juli 2025, IT-Modernisierung zwischen Legacy. Cloud und KI, <https://www.luenendonk.de/produkt/luenendonk-studie-it-modernisierung-zwischen-legacy-cloud-und-ki/>, letzter Zugriff am 05.10.2026

84: Europäische Kommission, 2026, The EU Open Source Strategy, <https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>, letzter Zugriff am 28.08.2026

85: Interview von A.-K. Nezik und M. Zydra mit Marietje Schaake: „Wir waren naiv.“ Erschienen in: Süddeutsche Zeitung, Nr. 40, 18.2.2026

- 86: Burwell, Frances & Propp, Kenneth (Atlantic Council), 14.01.2026, <https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/>, letzter Zugriff 31.08.2026
- 87: Bria, F.; Timmers, P.; Gernone, F., 2025, EuroStack – A European Alternative for Digital Sovereignty. Bertelsmann Stiftung, Gütersloh (127 Seiten)
- 88: Europäische Kommission, 2026, Strengthening Europe's Tech Sovereignty, <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty>, letzter Zugriff am 05.10.2026
- 89: Europäische Kommission, 03. Juni 2026, Chips Act 2.0, <https://digital-strategy.ec.europa.eu/en/policies/chips-act-2>, letzter Zugriff am 05.10.2026
- 90: zdf heute: Digitale Sicherheit: „Hilflos und kopflos“. Mit Markus Beckedahl im moma am 11.11.2025, <https://www.zdfheute.de/video/zdf-morgenmagazin/digital-sicherheit-investitionen-beckedahl-100.html>, letzter Zugriff 8.10.2026
- 91: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V., Dezember 2020, Grundsatzerklärung des Bitkom zur Verschlüsselung, https://www.bitkom.org/sites/main/files/2020-12/201211_pp_bitkom_grundsatzerklärung-verschlüsselung_0.pdf, letzter Zugriff am 31.08.2026
- 92: UP KRITIS, 01.12.2022, Empfehlungen zu Entwicklung und Bereitstellung von in Kritischen Infrastrukturen eingesetzten Produkten, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-entwicklung-einsatz-produkte.pdf?__blob=publicationFile&v=13, letzter Zugriff 31.08.2026
- 93: Bundesamt für Sicherheit in der Informationstechnik, NIS-2-regulierte Unternehmen, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html, letzter Zugriff 28.08.2026
- 94: Europäische Union, 14.12.2022, Amtsblatt der Europäischen Union – Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554>, letzter Zugriff am 28.08.2026
- 95: Bundesamt für Sicherheit in der Informationstechnik, 2026, Quantentechnologien und quantensichere Kryptografie, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html, letzter Zugriff 28.08.2026
- 96: CISA Helmholtz Center for Information Security, Post-Quantum Cryptography, <https://cisa.de/en/research/research-areas/algorithmic-foundations-and-cryptography/post-quantum-cryptography>, letzter Zugriff am 28.08.2026
- 97: Bundeswehr, 05.06.2025, Partnerschaft von BWI und Google: Die Bundeswehr bekommt eine eigene Cloud, <https://www.bundeswehr.de/de/meldungen/partnerschaft-bwi-google-bundeswehr-eigene-cloud-5952950>, letzter Zugriff am 28.08.2026

98: Europäische Kommission, 2026, The EU Open Source Strategy, <https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>, letzter Zugriff am 31.08.2026

99: Europäische Kommission, 15.12.2025, Data Act explained, <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>, letzter Zugriff 31.08.2026

100: Bundesanstalt für Finanzdienstleistungsaufsicht, 01.02.2024, BaFin veröffentlicht Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2024/meldung_2024_02_01_Cloud_Anbieter.html, letzter Zugriff 31.08.2026

101: Bundesamt für Sicherheit in der Informationstechnik, 10.04.2025, Strategiepapier "Sichere Softwarelieferketten", <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ZenDiS/Strategiepapier-Softwarelieferketten.com>, letzter Zugriff 31.08.2025

102: DER SPIEGEL (online), 18.12.2020, SolarWinds-Hack: Der Spionagefall des Jahres, <https://www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-der-spionagefall-des-jahres-a-0b728cc4-d375-4cb9-9450-3635ca8172a0>, letzter Zugriff 31.08.2026

Wirtschaft

103: Bitkom e. V., 18.09.2025, Wirtschaftsschutz 2025, <https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf>, letzter Zugriff am 28.08.2026

104: ARTE, 18.08.2026, Droht der digitale Blackout? KI und Internet am Limit, <https://www.ardmediathek.de/tv-programm/6a3be32d919d6d54b6e97e65>, letzter Zugriff am 28.08.2026

105: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2026, Kritische Infrastrukturen, https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html, letzter Zugriff am 28.08.2026

106: Bria, F.; Timmers, P.; Gernone, F., 2025, EuroStack – A European Alternative for Digital Sovereignty. Bertelsmann Stiftung, Gütersloh (127 Seiten).

107: Europäische Kommission, Oktober 2025, Cloud Sovereignty Framework, https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf, letzter Zugriff am 31.08.2026

108: Cloud Security Alliance, 05.06.2026, EU Tech Sovereignty: Cloud Concentration Risk and the Compliance Cascade, <https://labs.cloudsecurityalliance.org/research/eu-tech-sovereignty-cloud-ai-enterprise-risk-v1-0-csa-styled/>, letzter Zugriff am 31.08.2026

109: Bertelsmann Stiftung, April 2025, Policy Brief „EuroStack: Sicherstellung der digitalen Souveränität Europas“, https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/EuroStack_PolicyBrief_final.pdf, letzter Zugriff 31.08.2026

110: Sovereign Tech Agency GmbH, 2026, Sovereign Tech Fund, <https://www.sovereign.tech/de/programme/fund>, letzter Zugriff am 13.08.2026

111: Europäische Kommission, 2026, Die Open-Source-Strategie der EU, <https://digital-strategy.ec.europa.eu/de/policies/open-source-strategy>, letzter Zugriff am 31.08.2026

112: Open Source Initiative, 10.02.2026, Europe's Open Source Opportunity: our vision for the EU Open Digital Ecosystems strategy, <https://opensource.org/blog/europes-open-source-opportunity-our-vision-for-the-eu-open-digital-ecosystems-strategy>, letzter Zugriff am 31.08.2026

113: Europäische Kommission – interoperable Europe, 2026, Open Source in Cities and Regions, <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/open-source-cities-and-regions>, letzter Zugriff am 31.08.2026

114: Europäische Kommission, 19.12.2025, European Digital Innovation Hubs, <https://digital-strategy.ec.europa.eu/en/policies/edihs>, letzter Zugriff am 31.08.2026

115: Zentrum für Digitale Souveränität der Öffentlichen Verwaltung GmbH (ZenDiS), 2026, Das ZenDiS Souveränitätspaket, <https://www.zendis.de/unser-angebot#beratung>, letzter Zugriff am 01.09.2026

116: Bundesministerium für Wirtschaft und Energie, Juni 2026, Digitale Souveränität von KMU, https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/digitale-souveraenitaet.pdf?__blob=publicationFile&v=10, letzter Zugriff am 01.09.2026

117: Bundesministerium für Forschung, Technologie und Raumfahrt, 2026, Transfer in die Praxis, https://www.bmfr.bund.de/DE/Forschung/TransferInDiePraxis/transferindiepraxis_node.html, letzter Zugriff am 05.10.2026

118: Bundesministerium für Wirtschaft und Energie, Juni 2026, Digitale Souveränität von KMU, https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/digitale-souveraenitaet.pdf?__blob=publicationFile&v=10, letzter Zugriff am 01.09.2026

119: Papp, János Tamás (Constitutional Discourse), 21.03.2025, Meta's GDPR Fine: Delayed Accountability, but Maybe a Shift Toward Real Consequences, <https://constitutionaldiscourse.com/metass-gdpr-fine-delayed-accountability-but-maybe-a-shift-toward-real-consequences>, letzter Zugriff am 01.09.2026

120: Europäische Union, 14. September 2022, Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreithbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022R1925-20221012>, letzter Zugriff am 07.10.2026

121: Europäisches Parlament, 24.04.2026, Digital Markets Act enforcement: State of play, [https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2025\)772826](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)772826), letzter Zugriff am 01.09.2026

122: Europäische Kommission, 2026, Legal framework of EU data protection, https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en, letzter Zugriff am 01.09.2026

123: Hertie School, 30.10.2024, Europe ventures forward: Getting the scaleup of cleantech right, <https://www.delorscentre.eu/en/publications/detail/publication/venture-capital-getting-the-scaleup-of-cleantech-right>, letzter Zugriff am 01.09.2026

124: Mustier, Jean Pierre (Systemic Risk Centre), 12.03.2026, Europe's savings glut won't finance its future until it backs its own scale-ups, <https://www.systemicrisk.ac.uk/europes-savings-glut-wont-finance-its-future-until-it-backs-its-own-scale-ups>, letzter Zugriff am 01.09.2026

125: Europäische Union, September 2024, The future of European competitiveness – Part A | A competitiveness strategy for Europe, [https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?](https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf)

filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf, letzter Zugriff am 01.09.2026

126: Elcano Royal Institute, 16.07.2026, Scaling needs scale: Europe's existential challenge,

<https://www.realinstitutoelcano.org/en/analyses/scaling-needs-scale-europes-existential-challenge/>, letzter Zugriff am 01.09.2026

Bildung & Gesellschaft

127: Muuß-Merholz, Jöran, Podcast „Auftrag:Aufbruch“, Digitale Souveränität im Schulsystem mit Markus Beckedahl und Andrea Franke, für das Online-Magazin „Plan BD“ des Forum Bildung Digitalisierung e. V., <https://www.forumbd.de/podcast/digitale-souveranitat-im-schulsystem/>, letzter Zugriff am 07.10.2026, CC BY 4.0

128: Thimm, Caja, 2/2023, Digitale Souveränität und personale Autonomie: Herausforderungen für eine Digitalpädagogik, Mediendiskurs, https://mediendiskurs.online/data/hefte/ausgabe/104/thimm_digitale_souveraenitaet_md104.pdf, letzter Zugriff am 07.10.2026

129: Heise Medien, 28.09.2025, Missing Link: Tech-Monopole gegen digitale Souveränität an Schulen, <https://www.heise.de/hintergrund/Missing-Link-Tech-Monopole-gegen-digitale-Souveraenitaet-an-Schulen-10671905.html>, letzter Zugriff am 07.10.2028

130: Landeshauptstadt München, 2026, Digitale Souveränität, <https://muenchen.digital/projekte/digitale-souver%C3%A4nit%C3%A4t.html>, letzter Zugriff am 07.10.2026

131: Forum Bildung Digitalisierung, 2025, Digitale Souveränität im Schulsystem, <https://www.forumbd.de/wp-content/uploads/2025/09/orientierungspapier-digitale-souveranitat-konfbd25.pdf>, letzter Zugriff am 07.10.2026

132: Landeshauptstadt München, 2026, Digitale Souveränität, <https://muenchen.digital/projekte/digitale-souver%C3%A4nit%C3%A4t.html>, letzter Zugriff am 07.10.2026

133: Kultusminister Konferenz, 2026, Bildung in der digitalen Welt, <https://www.kmk.org/bildungsministerkonferenz/bildungsthemen/bildung-in-der-digitalen-welt.html>, letzter Zugriff am 07.10.2026

134: Forum Bildung Digitalisierung, 2025, Digitale Souveränität im Schulsystem, <https://www.forumbd.de/wp-content/uploads/2025/09/orientierungspapier-digitale-souveranitat-konfbd25.pdf>, letzter Zugriff am 07.10.2026

135: Heise Medien, 28.09.2025, Missing Link: Tech-Monopole gegen digitale Souveränität an Schulen, <https://www.heise.de/hintergrund/Missing-Link-Tech-Monopole-gegen-digitale-Souveraenitaet-an-Schulen-10671905.html>, letzter Zugriff am 07.10.2026

136: Forum Bildung Digitalisierung, 2025, Digitale Souveränität im Schulsystem, S. 3, <https://www.forumbd.de/wp-content/uploads/2025/09/orientierungspapier-digitale-souveranitat-konfbd25.pdf>, letzter Zugriff am 07.10.2026

137: Bundeszentrale für politische Bildung, 01. März 2024, Das Geschäftsmodell von Social-Media-Unternehmen, <https://www.bpb.de/themen/medien-journalismus/soziale-medien/545978/das-geschaeftsmodell-von-social-media-unternehmen/>, letzter Zugriff am 07.10.2026

138: Bundeszentrale für politische Bildung, 15. März 2023, Nachbarschaftsplattformen – Mehr als ein Geschäftsmodell?, <https://www.bpb.de/lernen/digitale-bildung/werkstatt/505129/nachbarschaftsplattformen-mehr-als-ein-geschaeftsmodell/>, letzter Zugriff am 07.10.2026

139: Bundeszentrale für politische Bildung, 23. September 2024, Quelle: Künstliche Intelligenz, Themenblätter im Unterricht, <https://www.bpb.de/shop/materialien/themenblaetter/552426/quelle-kuenstliche-intelligenz/>, letzter Zugriff am 07.10.2026

140: Niedersächsisches Kultusministerium, März 2026, Handreichung: Schule auf dem Weg der Bildung in der digital geprägten Welt, S. 20-22, https://wp.ratsgymnasium-row.de/wp-content/uploads/2026/05/Handreichung_Digitalitaet_Band_2_V1.0.pdf, letzter Zugriff am 07.10.2026

141: Forum Bildung Digitalisierung, 2025, Digitale Souveränität im Schulsystem, S. 2-3, <https://www.forumbd.de/wp-content/uploads/2025/09/orientierungspapier-digitale-souveranitat-konfbd25.pdf>, letzter Zugriff am 07.10.2026

142: Goldacker, Gabriele (Kompetenzzentrum Öffentliche Informationstechnologie), November 2017, Digitale Souveränität, S.5, <https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet/Digitale%20Souver%c3%a4nit%c3%a4t.pdf>, letzter Zugriff am 07.10.2026

143: Netzwerk Datenschutzexpertise, 11. Dezember 2024, Ein Recht auf analoge Teilhabe - Freiheit vor Digitalzwang, Praktische und rechtliche Aspekte, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2024_digitalzwang3.pdf, letzter Zugriff am 07.10.2026

144: Digitalcourage, 2026, Digitalzwang, <https://digitalcourage.de/digitalzwang>, letzter Zugriff am 07.10.2026

145: Deutsche Stiftung Verbraucherschutz, 2026, Medien und Information, <https://www.verbraucherstiftung.de/themen/medien>, letzter Zugriff am 07.10.2026

146: Bayerischer Rundfunk, 06. Mai 2026, Warum SPD, Grüne und Linke die Plattform X verlassen, <https://www.br.de/nachrichten/deutschland-welt/warum-spd-gruene-und-linke-die-plattform-x-verlassen,VllsyKT>, letzter Zugriff am 07.10.2026

147: Save Social, 2026, Soziale Netzwerke als demokratische Kraft retten, <https://savesocial.eu/de/>, letzter Zugriff am 07.10.2026

148: Bundeszentrale für politische Bildung, 19. März 2026, Das Fediverse als Raum politischer Bildung, <https://www.bpb.de/lernen/digitale-bildung/werkstatt/576352/das-fediverse-als-raum-politischer-bildung/>, letzter Zugriff am 07.10.2026

149: Bundeszentrale für politische Bildung, 01. März 2024, Getriebene der Plattformen – Wie etablierte Medien ihr Geschäft den Social-Media-Plattformen angepasst haben, <https://www.bpb.de/themen/medien-journalismus/soziale-medien/545983/getriebene-der-plattformen/>, letzter Zugriff am 07.10.2026

150: Bundeszentrale für politische Bildung, 2023, Newsletter als Fundraising-Tool, <https://www.bpb.de/die-bpb/foerderung/akquisos/524302/newsletter-als-fundraising-tool/>, letzter Zugriff am 07.10.2026

151: Digitale Zivilgesellschaft, 2026, Digitalvisionen, <https://digitalezivilgesellschaft.org/digitalvisionen/>, letzter Zugriff am 07.10.2026

152: Open Source Business Alliance, 05. Oktober 2026, Digitale Souveränität gemeinsam denken: Neue Veranstaltungsreihe bringt Verwaltung, Wirtschaft und IT-Praxis deutschlandweit ins Gespräch, <https://osb-alliance.de/featured/digitale-souveraenitaet-gemeinsam-denken-neue-veranstaltungsreihe-bringt-verwaltung-wirtschaft-und-it-praxis-deutschlandweit-ins-gespraech>, letzter Zugriff am 07.10.2026

153: Bundesrat, 16. September 2026, Unterrichtung durch die Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Cloud- und KI-Ökosystems, Drucksache 536/26, <https://dserver.bundestag.de/brd/2026/0536-26.pdf>, letzter Zugriff am 07.10.2026

154: Strasmann, Jan Frederik, 25. April 2026, Recht auf informationelle Selbstbestimmung: Bedeutung im Datenschutz, VFR Verlag für Rechtsjournalismus GmbH, <https://www.datenschutz.org/recht-auf-informationelle-selbstbestimmung/>, letzter Zugriff am 07.10.2026

155: Mühlhoff, Rainer, 2023, Die Macht der Daten – Osnabrücker Universitätsreden, Band 10, Universitätsverlag Osnabrück, https://rainermuehlhoff.de/media/publications/m%C3%BChlhoff_2023_die_macht_der_daten.pdf, letzter Zugriff am 07.10.2026

156: Goldacker, Gabriele (Kompetenzzentrum Öffentliche Informationstechnologie), November 2017, Digitale Souveränität, S. 5, <https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet/Digitale%20Souver%c3%a4nit%c3%a4t.pdf>, letzter Zugriff am 07.10.2026

157: Mühlhoff, Rainer, 2023, Die Macht der Daten – Osnabrücker Universitätsreden, Band 10, Universitätsverlag Osnabrück, https://rainermuehlhoff.de/media/publications/m%C3%BChlhoff_2023_die_macht_der_daten.pdf, letzter Zugriff am 07.10.2026

158: Autoriteit Persoonsgegevens, 09. April 2025, Right to human intervention in decision-making processes, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/privacy-rights-under-the-gdpr/right-to-human-intervention-in-decision-making-processes>, letzter Zugriff am 08.10.2026

159: European Data Protection Board, 04. Mai 2020, Guidelines 05/2020 on consent under Regulation 2016/679, https://www.edpb.europa.eu/documents/guideline/guidelines-052020-on-consent-under-regulation-2016679_en , letzter Zugriff am 08.10.2026

160: European Digital Rights (EDRi), 2026, Advocating for better policy, <https://edri.org/what-we-do/policy/>, letzter Zugriff am 08.10.2026

161: European Data Protection Board, 20. Oktober 2020, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en, letzter Zugriff am 08.10.2026

Bildnachweise

- ©jamestehArt.via Canva.com (Titelseite)
- ©KanawatTH via Canva.com (s. Vorwort *Maßnahmenpapier*)
- ©Hans von Pixabay via Canva.com (s. Vorwort *Säulen*)
- ©geralt von Pixabay via Canva.com (S. 1 u. 2)
- ©Edward Olive via Canva.com (S. 10 u. 11)
- ©Diaconescu Vlad's Images via Canva.com (S. 23, 24 u. 27)
- ©afloimages via Canva.com (S. 31 u. 32)
- ©TrueCreatives via Canva.com (S. 41 u. 42)

MASSNAHMENPAPIER

Die **gemeinnützige Gesellschaft cum ratione** realisiert Projekte zu nachhaltigem Leben und Wirtschaften sowie zur Sicherung unserer Demokratie. Thematisch reichen diese unter anderem von Fairen Textilien über Energie und Verkehr bis hin zu Wohnen und Bauen sowie der Sicherung unserer Demokratie durch einen Handlungsfähigen Staat und Digitale Souveränität. Aufbauend auf den drei etablierten Säulen der Nachhaltigkeit – Ökologie, Soziales und Ökonomie – vertreten wir die Auffassung, dass Sicherheitspolitik als vierte Dimension der Nachhaltigkeit anerkannt werden sollte. Alle unsere Projekte sind darauf ausgerichtet, einen langfristigen gesellschaftlichen Mehrwert zu schaffen.

Das **Software Innovation Lab** der Universität Paderborn ist ein interdisziplinäres Forschungsinstitut, das sich mit zentralen Fragestellungen und Auswirkungen der digitalen Transformation befasst. Im Kontext des SICP – Software Innovation Campus Paderborn erforscht es gemeinsam mit seinen Partnern innovative und nachhaltige software- und datengetriebene Lösungen.