Policy Brief:

Digitale Souveränität in Europa

Definition, Status, Handlungsoptionen

Version 3
November 2026

4future.institute Policy Brief Series
Policy Brief Nr. 2026-001 (DE)
ISSN 3061-1881 (Online)
DOI: 10.5281/zenodo.24042085

Werner Illsinger
Executive Director
4future.institute
werneri@4future.institute

Impressum

4future.institute · Graben 17/10 · 1010 Wien · Österreich · Telefon: +43 1 31440-0 · hello@4future.institute

4future.institute ist Teil der 4future.group und organisatorisch als unabhängige Einheit in der 4future business GmbH angesiedelt.

Firmenbuchnummer: FN 459359 d · Firmenbuchgericht: Handelsgericht Wien · UID-Nummer: ATU71656745 · Mehrheitseigentümerin: 4future.foundation

Über das 4future.institute: Zu fast jedem relevanten Thema unserer Zeit gibt es mehr Meinungen als Orientierung. Das 4future.institute fragt: Was stimmt hier eigentlich, was sind die strukturellen Bedingungen — und macht das Sinn, nicht nur wirtschaftlich, sondern für uns als Gesellschaft? Sein Orientierungsrahmen ist das 4future-Haus: Ziel ist ein gutes Leben für alle, heute und für kommende Generationen. Getragen wird es von drei Säulen, den drei V — Veränderung von Arbeit und Wirtschaft, Verteilungsgerechtigkeit und Versorgungssicherheit —, verbunden durch Rechtsstaat, bürgernahe Verwaltung und Koordination und gegründet auf europäische Grundwerte, Ethik und Nachhaltigkeit (Leitpapier „Strategie für eine lebenswerte Zukunft“, 4future.institute Papers Nr. 2026-001). Digitale Souveränität ist Teil der Versorgungssicherheit: digitale Dienste verlässlich nutzen, Anbieter wechseln und über eigene Daten entscheiden zu können. Die 4future.foundation ermöglicht die unabhängige Arbeit des Instituts; finanzielle Unterstützung begründet keinen Einfluss auf Inhalte oder Schlussfolgerungen.

Reihe: 4future.institute Policy Brief Series, Nr. 2026-001 (DE), ISSN 3061-1881 (Online), ,
DOI: https://doi.org/10.5281/zenodo.24042085

Sprachfassungen: Engli sche Fassung: Policy Brief No. 2026-001 (EN). Bei Abweichungen ist die deutsche Fassung maßgeblich.

Offenlegung: Werner Illsinger ist Executive Director des 4future.institute, Geschäftsführer der 4future business GmbH und Vorstandsvorsitzender der 4future.foundation. Er hat zudem 4future.digital aufgebaut und ist dort als CTO tätig; 4future.digital bietet Cloud- und Kollaborationsdienste als europäische Alternative zu Microsoft 365 und Google Workspace an. 4future.digital ist derzeit ein eigenständiges Unternehmen; Ziel ist, dass es wie die 4future business GmbH eine Tochter der 4future.foundation wird. Die 4future business GmbH erbringt selbst keine Cloud-Dienste. Empfehlungen des Instituts sind anbieterneutral formuliert; 4future.digital und seine Dienste werden in diesem Papier weder genannt noch bewertet.

Executive Summary

Der Anteil der EU-27 am weltweiten nominalen BIP ist seit 1990 von rund 27 % auf rund 18 % gesunken. Der Anteil der USA blieb mit rund 26 % annähernd stabil, China wuchs von unter 2 % auf knapp 17 %. Ein sinkender Anteil bedeutet keinen absoluten Rückgang: Die europäische Wirtschaft ist gewachsen, aber langsamer als andere. Diese Entwicklung hat viele Ursachen. Dieses Papier untersucht eine davon, die politisch gestaltbar ist: Was Europa an Daten, Nutzern und Märkten hervorbringt, wird zu einem erheblichen Teil in den Bilanzen nicht-europäischer Plattformunternehmen zu Wertschöpfung. Dieses Papier analysiert, warum — und was sich ändern muss.

Die grundlegende digitale Infrastruktur Europas — Cloud, Identität, Kommunikation, KI — wird fast vollständig von Plattformen bereitgestellt, die fremden Rechtsordnungen unterliegen und monopolartige Marktstrukturen aufweisen. Sie unterliegen damit konkurrierenden Rechtsansprüchen, deren Folgen europäische Kunden weder vollständig kontrollieren noch zuverlässig ausschließen können; eine rechtlich zulässige Nutzung beseitigt diese Abhängigkeit nicht.

Daraus entsteht ein strukturelles Defizit in drei Dimensionen: Rechtlich können europäische Kunden Zugriffe nach US-Recht wie dem CLOUD Act und FISA Section 702 weder kontrollieren noch ausschließen. Technologisch begrenzt die Dominanz proprietärer Multi-Tenant-Architekturen Prüfbarkeit und Wechselbarkeit. Ökonomisch fließt ein erheblicher Teil der digitalen Wertschöpfung aus Europa ab.

Die Entwicklungen seit Erstpublikation dieses Papiers haben die Lage verschärft: Der PCLOB — eine zentrale Aufsichtsinstitution, auf die sich das EU-US Data Privacy Framework stützt — ist seit der Entlassung seiner demokratischen Mitglieder im Januar 2025 nicht mehr beschlussfähig.

FISA Section 702 ist nach zwei kurzfristigen Verlängerungen im April am 12. Juni 2026 ausgelaufen — erstmals seit seiner Einführung 2008. Bestehende Genehmigungen gelten bis zu ihrem Ablauf, voraussichtlich im März 2027, unter fortbestehender Aufsicht des FISA-Gerichts weiter. Danach wäre ohne Neuregelung für Überwachung, die bisher auf Section 702 gestützt wurde, grundsätzlich eine Einzelanordnung nach Titel I des FISA erforderlich. Eine dauerhafte Regelung steht zum Zeitpunkt der Veröffentlichung aus. Die Rechtsgrundlage, auf die sich die Bewertung des US-Schutzniveaus im Data Privacy Framework stützt, ist damit in Bewegung.

Das DPF ist vor dem Europäischen Gerichtshof angefochten (Rs. C-703/25 P). Industriereaktionen wie die EU Data Boundary von Microsoft und die AWS European Sovereign Cloud verbessern Datenresidenz und operative Kontrolle in Europa, beseitigen aber nicht das Problem konkurrierender Rechtsansprüche aus Drittstaaten (Abschnitt 2.2).

Wie weit Rechtskonformität und nachweisbarer Schutz auseinanderfallen, zeigt der Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu Microsoft 365 vom November 2025: Er hält eine Erfüllung der vertraglichen Anforderungen an die Weisungsbindung für möglich, obwohl er festhält, dass Microsoft eine Offenlegung auf Anordnung der US-Regierung nicht vollständig ausschließen kann. Die positive Vertragsbewertung beantwortet damit die entscheidende Frage des Kunden nicht: Sind meine Daten gegen einen solchen Zugriff tatsächlich geschützt? (Abschnitt 2.1)

Am 3. Juni 2026 hat die Europäische Kommission den Cloud and AI Development Act (CADA) vorgeschlagen — den ersten Versuch, im Unionsrecht festzulegen, was eine souveräne Cloud ist. Das ist ein Schritt in die richtige Richtung; ob er sein Ziel erreicht, entscheidet das Gesetzgebungsverfahren (Abschnitt 2.4).

Was dieses Papier beiträgt. Dieses Papier ergänzt bestehende Analysen in vier Punkten:

- **Das Datenschutz-Trilemma:** Der Konflikt zwischen europäischem Datenschutzrecht und US-Cloud-Diensten ist struktureller, nicht politischer Natur. Der Verantwortliche bleibt nach Art. 5 Abs. 2 und Art. 28 DSGVO rechenschaftspflichtig, kann die Verarbeitung in der Praxis nur anhand von Prüfberichten kontrollieren, die der Anbieter selbst beauftragt, und kann ein entscheidendes Risiko weder durch Audits noch durch Verträge ausschließen: behördliche Zugriffe nach dem Recht eines Drittstaats, die mit Verschwiegenheitspflichten verbunden sein können. Bei Microsoft 365 schränkt eine Verschlüsselung, die den Anbieter wirksam ausschließt, zugleich zentrale Funktionen des Dienstes erheblich ein. Dieser Konflikt besteht unabhängig von der politischen Lage in den USA (Abschnitt 2.1).
- **Ein unabhängiger Maßstab:** CADA wird an Zertifizierungskriterien gemessen, die dieses Papier vor Veröffentlichung des Vorschlags formuliert hat (Abschnitt 3.1.2; Version 2 vom 1. Juni 2026) — nicht an Compliance-Pflichten für Anbieter oder an den Interessen einzelner Marktteilnehmer.
- **Befunde aus dem Gesetzestext:** Auf Grundlage des Vorschlags, seiner Anhänge und der Folgenabschätzung zeigt dieses Papier, dass die Basisstufe eine Souveränitätsbezeichnung vergibt, ohne Zugriffe von Drittstaaten auf Kundendaten zu verhindern; dass die Pflicht zu höheren Stufen an Sektor und Tätigkeit statt an die verarbeiteten Daten anknüpft, wodurch horizontale Büro-, Kollaborations-, E-Mail- und Identitätsplattformen systematisch unterschätzt werden; dass Folgenabschätzung und Gesetzestext bei der Frage auseinanderfallen, ob aus Drittstaaten kontrollierte Anbieter Stufe 3 erreichen können; und dass die Schätzung der Kommission zur Verteilung der Anwendungsfälle auf einer schmalen empirischen Basis beruht — Punkte, die in den in Abschnitt 2.4 ausgewerteten Analysen nicht behandelt werden.

- **Digitale und energetische Souveränität:** Große Rechenzentren nicht-europäischer Anbieter schaffen vor Ort wenige dauerhafte Arbeitsplätze, während die wertschöpfenden Funktionen am Sitz des Betreibers verbleiben; zugleich kann ihr Strombedarf die Abhängigkeit von importierten fossilen Energieträgern vertiefen, sofern er nicht durch zusätzliche erneuerbare Erzeugung gedeckt wird. Am Fallbeispiel Kronstorf argumentiert dieses Papier, dass digitale Souveränität nicht auf Kosten energetischer Souveränität angestrebt werden darf, und schlägt eine Zusätzlichkeitspflicht nach dem Vorbild der irischen Netzanschlussregelung von 2025 vor (Abschnitte 2.3 und 3.3.5).

Ergänzend vertieft das Begleitpapier „Digitale Souveränität braucht überprüfbare Interoperabilität“ (Juni 2026) die Frage, ob sich Dienste praktisch ersetzen lassen. Dieses Papier greift dessen Vorschlag einer europäischen Interoperabilitätszertifizierung auf und verbindet ihn mit den Stufen des CADA (Abschnitte 2.4 und 3.2.2).

In zentralen digitalen Funktionen fehlt Europa derzeit die wirksame Kontrolle über wesentliche Abhängigkeiten — rechtlich, technologisch und ökonomisch.

Der Weg dorthin erfordert einen systemischen Ansatz: einen durchsetzbaren Rechtsrahmen, auditierbare europäische Cloud- und KI-Infrastrukturen, verbindliche Interoperabilitätsstandards, strategische Digitalinvestitionen und ein Bildungssystem, das kritisches Denken fördert. Diese Maßnahmen verursachen Kosten. Ihnen stehen vermiedene Abhängigkeits- und Ausfallrisiken sowie ein erwarteter Nutzen für Resilienz, Wettbewerb und europäische Wertschöpfung gegenüber; in diesem Sinn sind sie eine Investition in Europas Zukunftsfähigkeit.

Inhaltsverzeichnis

Executive Summary 3

1 Begriffsklärung: Digitale Souveränität 9

1.1 Juristische Souveränität 10

1.2 Technologische Souveränität 10

1.3 Ökonomische und gesellschaftliche Souveränität 10

2 Status der digitalen Souveränität in Europa 11

2.1 Rechtlicher Status: Widersprüchliche Rechtsordnungen und strukturelle Konflikte 11

2.2 Technologischer Status: Abhängigkeit von nicht-europäischen Plattformen 19

2.3 Ökonomischer Status: Wertschöpfungsverlust und strategische Verwundbarkeit 22

2.4 Politische Entwicklungen: Der Cloud and AI Development Act (CADA) 25

2.4.1 Bewertung anhand der Anforderungen dieses Papiers 29

3 Handlungsoptionen zur Stärkung der digitalen Souveränität 34

3.1 Rechtlicher Rahmen 34

3.1.1 Anwendbares Recht klar definieren 34

3.1.2 EU-weite Zertifizierung von Cloud- und KI-Diensten 34

3.1.3 Neuverhandlung transatlantischer Abkommen 36

3.1.4 Rechtsrahmen für kritische digitale Infrastruktur 37

3.1.5 Globale Regulierung multinationaler Konzerne etablieren 37

3.2 Technologischer Rahmen: Aufbau europäischer Kontrollfähigkeit 37

3.2.1 Aufbau einer europäischen Cloud- und KI-Infrastruktur 37

3.2.2 Interoperabilität als verbindliche Grundlage 38

3.2.3 Europäische Identitäts- und Vertrauensdienste 39

3.2.4 Europäische Sicherheitsarchitektur 40

3.3 Ökonomischer Rahmen: Marktmechanismen neu gestalten 40

3.3.1 Strategische europäische Digitalinvestitionen / Innovation 40

3.3.2 Reduktion wirtschaftlicher Abhängigkeiten 41
3.3.3 Markt 42
3.3.4 Europäische Beschaffungsreform 43
3.3.5 Energiepflichten für große Rechenzentren 44
3.4 Gesellschaftlicher Rahmen: Kompetenz, Transparenz und Teilhabe 46
3.4.1 Bildung als Basis 46
3.4.2 Transparenz als Grundvoraussetzung für Vertrauen 48
3.4.3 Europäischer Talent-, Forschungs- und Innovationsaufbau 48
3.4.4 Zivilgesellschaftliche Beteiligung an digitalen Großprojekten 48
3.4.5 Globale Kooperation stärken 49
4 Fazit 50
5 Call to Action 51
I. Anhang: Über den Autor 52
II. Anhang: Begriffsbestimmungen 53
III. Anhang: Quellen & Literatur 55
Rechtliche Grundlagen 55
Marktdaten & wirtschaftliche Fakten 55
Technische Grundlagen 55
Politische Debatten & Think-Tank-Analysen 55
Bildung, Kompetenzen & Gesellschaft 55
Entwicklungen 2025–2026 56

1 Begriffsklärung: Digitale Souveränität

Digitale Souveränität bezeichnet die Fähigkeit von Staaten, Institutionen, Unternehmen und Individuen, digitale Technologien, Daten, Infrastrukturen und Kommunikationssysteme **eigenständig, rechtskonform und sicher zu betreiben oder über deren Nutzung frei zu entscheiden**. Der Begriff umfasst drei zentrale Dimensionen: juristische, technologische sowie ökonomisch-gesellschaftliche Souveränität.

Digitale Souveränität bedeutet jedoch **nicht**, dass Europa alle Technologien selbst herstellen oder betreiben muss. Es geht **nicht** um Autarkie.

Es geht darum, **dass wir selbst bestimmen können**, wem wir vertrauen, welche Technologien wir einsetzen und unter welchen rechtlichen Rahmenbedingungen diese betrieben werden.

Selbstbestimmung erfordert:

- **Verlässliche Partner**, deren Unternehmen in einem Rechtsraum agieren, der mit europäischen Grundrechten kompatibel ist.
- **Technische Kontrollmöglichkeit**, die es erlaubt, Versprechen zu überprüfen.
- **Pluralität statt Monopole** – denn Selbstbestimmung ist ausgeschlossen, wenn ein einzelner Anbieter (auch ein europäischer) faktisch alternativlos ist.
- **Gestaltbare, transparente Abhängigkeiten**, die nicht durch extraterritoriale Gesetze oder proprietäre Lock-ins erzwungen werden.

Digitale Souveränität bedeutet nicht Abschottung oder technologische Autarkie.

Europa muss nicht alle Technologien selbst bauen – aber es muss frei entscheiden können, *welche Systeme eingesetzt werden*, und sicherstellen, dass diese Systeme in einem **kompatiblen Rechtsraum**, nach **transparenter Governance** und ohne **monopolartige Abhängigkeiten** betrieben werden.

Digitale Souveränität ist daher kein nationalistisches oder protektionistisches Konzept, sondern ein Prinzip **rechtlicher Kompatibilität, Wettbewerbsoffenheit und selbstbestimmter Partnerwahl**.

Digitale Souveränität bedeutet somit: Freiheit in der Wahl, Kontrolle über die Grundlagen und Sicherheit über den Rechtsraum – nicht Abschottung oder Isolation.

Digitale Souveränität ist nicht losgelöst von energetischer Souveränität und ökologischer Nachhaltigkeit zu erreichen. Eine digitale Infrastruktur, die die Abhängigkeit von importierten fossilen Energieträgern vertieft oder Boden, Wasser und erneuerbare Kapazitäten verbraucht, ohne zu deren Ausbau beizutragen, ersetzt lediglich eine strategische Abhängigkeit durch eine andere.

1.1 Juristische Souveränität

Die Fähigkeit eines Staates, einer Organisation oder eines Betreibers, sicherzustellen, dass digitale Systeme und Daten ausschließlich den Rechtsordnungen unterliegen, denen sie aufgrund ihrer geographischen, organisatorischen und rechtlichen Zugehörigkeit unterliegen sollen – ohne unbeabsichtigte oder extraterritoriale Zugriffsbefugnisse fremder Staaten.

- Transparenz über Zugriffe staatlicher Stellen
- Rechtsschutz der Betroffenen
- Ausschluss extraterritorialer Zugriffsbefugnisse fremder Staaten

1.2 Technologische Souveränität

Die Fähigkeit, digitale Systeme, Software und Infrastruktur unabhängig zu entwickeln, zu betreiben oder zu wechseln. Dazu gehören:

- Kontrolle über Architektur, Datenflüsse und Kryptografie
- Interoperabilität und Standardisierung
- Vermeidung kritischer Abhängigkeiten von einzelnen Anbietern
- Resilienz gegenüber Störungen oder politischen Maßnahmen

1.3 Ökonomische und gesellschaftliche Souveränität

Die Fähigkeit von Wirtschaft und Gesellschaft, digitale Technologien:

- eigenständig anzuwenden
- zu verstehen
- und unabhängig weiterzuentwickeln

Digitale Souveränität ist damit kein rein technisches Konzept, sondern ein staatliches und wirtschaftliches **Fähigkeitsniveau**, das Rechtsstaatlichkeit, Wettbewerbsfähigkeit und Sicherheit in der digitalen Welt gewährleistet.

2 Status der digitalen Souveränität in Europa

Die Analyse der aktuellen Lage zeigt Defizite in allen Dimensionen digitaler Souveränität – rechtlich, technologisch und ökonomisch.
Diese Defizite entstehen nicht durch Einzelentscheidungen, sondern durch strukturelle Rahmenbedingungen:
extraterritoriale Rechtsordnungen, proprietäre Plattformarchitekturen und globale Marktkonzentration. In Kombination führen sie dazu, dass Europa zentrale digitale Funktionen nicht unabhängig steuern kann.

2.1 Rechtlicher Status: Widersprüchliche Rechtsordnungen und strukturelle Konflikte

Europa befindet sich in einem systemischen Konflikt, der sich aus drei Faktoren ergibt:

- **Europäisches Datenschutzrecht:**
  Die DSGVO verlangt, dass europäische Verantwortliche die volle Kontrolle über personenbezogene Daten behalten –
  einschließlich Schutz vor unbefugten staatlichen Zugriffen.
- **US-amerikanische Gesetze mit extraterritorialer Wirkung:**
  Gesetze wie der CLOUD Act und FISA 702 verpflichten US-Unternehmen, Daten herauszugeben –
  auch wenn diese physisch in der EU gespeichert sind und europäischen Regelungen unterliegen.
- **Technische Struktur moderner Cloudsysteme:**
  Multi-Tenant-Architekturen begrenzen die unmittelbare technische Kontrolle durch europäische Kunden; Kunden erhalten in der Regel nur Prüfberichte von Auditoren, die der Anbieter selbst beauftragt.

Der Europäische Gerichtshof hat in **Schrems II (C-311/18)** den Privacy Shield für ungültig erklärt, weil das US-Recht — insbesondere FISA Section 702 — kein dem Unionsrecht im Wesentlichen gleichwertiges Schutzniveau gewährleistete und Betroffenen keinen wirksamen Rechtsbehelf bot. Standardvertragsklauseln blieben gültig, setzen aber eine Prüfung im Einzelfall und gegebenenfalls zusätzliche Maßnahmen voraus. Ein generelles Verbot der Nutzung von US-Cloud-Diensten folgt aus dem Urteil nicht; seit Juli 2023 sind Übermittlungen an nach dem Data Privacy Framework zertifizierte Unternehmen auf Grundlage eines Angemessenheitsbeschlusses zulässig. Die folgende Analyse unterscheidet daher vier Ebenen, deren Erfüllung einander nicht wechselseitig belegt: die rechtliche Zulässigkeit (darf die Verarbeitung stattfinden?), die Wirksamkeit von Schutzmaßnahmen (welches Risiko wird tatsächlich verringert?), die praktische Kontrollfähigkeit (kann der betroffene Kunde die Maßnahmen nutzen, überprüfen und durchsetzen?) und die digitale Souveränität (kann er seine wesentlichen digitalen Funktionen auch bei Konflikten, Ausfällen oder einem notwendigen Anbieterwechsel aufrechterhalten?). Maßstab ist dabei die praktische Nutzbarkeit: Eine Schutzmaßnahme begründet erst dann Kontrollfähigkeit, wenn der betroffene Kunde sie tatsächlich einsetzen, ihre Wirksamkeit überprüfen und ihren Einsatz finanzieren kann.

Wie leicht diese Ebenen in der Praxis verschwimmen, zeigt der Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) zu Microsoft 365 vom November 2025. Er prüft das Vertragswerk anhand der 2022 von der Datenschutzkonferenz erhobenen Kritikpunkte und kommt zum Ergebnis, dass ein datenschutzkonformer Betrieb möglich ist, sofern auch die Kunden ihre Pflichten als Verantwortliche erfüllen. Technische Prüfungen liegen dem Bericht nicht zugrunde; Fragen der digitalen Souveränität behandelt er ausdrücklich nicht (S. 9). Bemerkenswert ist, was der Bericht selbst festhält: Microsoft habe eingeräumt, dass eine Offenlegung auf Anordnung der US-Regierung ohne ausdrückliche Zustimmung des Verantwortlichen künftig nicht vollständig ausgeschlossen werden kann; der HBDI verweist dafür auf die Anhörung vor dem französischen Senat (S. 67 f.). Unmittelbar im Anschluss stellt er fest, dass der Anforderung der Weisungsbindung nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a DSGVO „entsprochen werden kann“ (S. 68). Der Bericht hält damit beides zugleich fest: Ein Zugriff auf Anordnung der US-Regierung ist nicht ausgeschlossen — und die Anforderung gilt dennoch als erfüllbar. Das Ergebnis stützt sich auf vertragliche Zusagen: Microsoft werde gegen solche Anordnungen rechtlich vorgehen und gegenüber hessischen öffentlichen Stellen die DSGVO auch dann einhalten, wenn ausländische Behörden ein abweichendes Verhalten erzwingen. Ob diese Zusagen im Ernstfall eingehalten werden, kann der Kunde nicht überprüfen. Der Bericht hält es zudem für „diskutabel“, ob ein IT-Dienstleister mit bedeutender Marktmacht sachgerecht als weisungsgebundener Auftragsverarbeiter eingeordnet werden kann, und sieht hier den Gesetzgeber gefordert (S. 46, Fn. 66). Folgerichtig empfiehlt er Verantwortlichen, in angemessenen Fällen eigene Audits und technische Prüfungen durchzuführen (S. 87) und stets alternative, möglichst europäische Lösungen zu evaluieren, zu dokumentieren und zu erproben, um die Abhängigkeit von einzelnen Anbietern und die Möglichkeiten politischen Drucks durch Drittstaatenakteure zu verringern (S. 93). Der Bericht beantwortet damit die Frage der Zulässigkeit auf Vertragsebene und benennt zugleich — ohne sie zu lösen — die Fragen der Kontrollfähigkeit und der Souveränität, um die es in diesem Papier geht.

Genau hier liegt der Kern des Datenschutz-Trilemmas: Eine positive Bewertung auf Vertragsebene beantwortet nicht, ob die Daten gegen einen Drittstaatenzugriff tatsächlich geschützt sind. Einen erfolgten Zugriff stellt der Bericht nicht fest — er macht die Kontrolllücke sichtbar.

Das folgende Schaubild zeigt das strukturelle Problem klar auf:
Nach Art. 5(2) und Art. 28 DSGVO trägt der *Auftraggeber (Kunde)* die volle Verantwortung für die rechtskonforme Verarbeitung personenbezogener Daten. Er muss sicherstellen – und nachweisen können –, dass der eingesetzte (Cloud-)Provider sämtliche Anforderungen der DSGVO erfüllt.

Um dieser Verantwortung nachzukommen, muss der Verantwortliche die Einhaltung durch den Auftragsverarbeiter überprüfen können: Art. 28 Abs. 3 lit. h DSGVO verpflichtet den Auftragsverarbeiter, Überprüfungen einschließlich Inspektionen zu ermöglichen, die vom Verantwortlichen oder einem von ihm beauftragten Prüfer durchgeführt werden. Das Prüfrecht liegt beim Kunden. In der Praxis ersetzen große Cloud-Anbieter dieses Recht durch Prüfberichte von Auditoren, die sie selbst beauftragen und deren Prüfumfang sie selbst festlegen. Microsoft etwa lässt seine Online-Dienste regelmäßig prüfen und stellt die Berichte im Service Trust Portal bereit, teils erst nach Annahme einer Geheimhaltungsvereinbarung.

Eine eigene Prüfung des Kunden sieht das allgemeine Datenschutz-Addendum von Microsoft nur vor, soweit dessen Prüfanforderungen durch diese Berichte nicht angemessen erfüllt werden können; Umfang und Zeitpunkt sind mit Microsoft zu vereinbaren, und der Kunde trägt sämtliche Kosten, einschließlich des Zeitaufwands von Microsoft zu dessen Dienstleistungssätzen. Welche Größenordnung das erreichen kann, zeigt beispielhaft eine von einem Microsoft-Partner veröffentlichte Fassung des Financial Services Amendment für Kunden des Finanzsektors: Sie setzt 4.000 US-Dollar pro Tag und eingesetzter Microsoft-Fachkraft an, zuzüglich Reisekosten — ein Beispiel für eine dokumentierte Vertragsgestaltung, kein allgemeiner aktueller Tarif. Das Vertragswerk gewährleistet kleinen Auftraggebern damit keine wirtschaftlich zugängliche eigene Prüfung; es überträgt Organisation und Finanzierung zusätzlicher Kontrolle auf Kunden — Gemeinden, Schulen, Vereine, KMU —, deren Ressourcen dafür regelmäßig begrenzt sind. Für die große Mehrheit der Verantwortlichen bleibt die Kontrolle damit faktisch auf das beschränkt, was der Anbieter zeigt. Und selbst eine eigene Prüfung könnte eines nicht belegen: das Ausbleiben behördlich angeordneter Herausgaben nach dem Recht eines Drittstaats. Solche Anordnungen können mit Verschwiegenheitspflichten verbunden sein und sind dann weder für den Kunden noch für einen Prüfer erkennbar.

Ergänzend verpflichtet sich der Anbieter in der **Auftragsverarbeiter-Vereinbarung (AVV)**, die DSGVO einzuhalten, und trägt nach Art. 28 und 32 DSGVO eigene Pflichten. Unterliegt er jedoch der US-Rechtsordnung, kann er **nicht rechtsverbindlich** zusichern, dass Herausgabeanordnungen nach US-Recht (z. B. CLOUD Act, FISA Section 702) unterbleiben; er kann sich lediglich verpflichten, solche Anordnungen anzufechten und den Kunden zu informieren, soweit dies rechtlich zulässig ist.

Häufig wird auf technische und organisatorische Maßnahmen verwiesen, vor allem auf Verschlüsselung. Entscheidend ist dabei, wer die Schlüssel besitzt und wer die Daten im Klartext verarbeitet. Verwaltet der Kunde zwar die Schlüssel, verwendet der Dienst sie aber selbst — etwa bei Microsoft Customer Key —, entschlüsselt der Anbieter die Daten zur Verarbeitung weiterhin; gegen eine an ihn gerichtete Herausgabeanordnung schützt das nicht. Schließt die Verschlüsselung den Anbieter dagegen wirksam aus, etwa bei Microsofts Double Key Encryption, verliert der Dienst genau die Funktionen, für die er genutzt wird: Solche Dokumente lassen sich in den Office-Web-Apps nicht anzeigen, gemeinsame Bearbeitung und automatisches Speichern werden nicht unterstützt, und KI-Funktionen wie Copilot können die Inhalte nicht verarbeiten. Bei Microsoft 365 schränkt eine Verschlüsselung, die Microsoft wirksam vom Inhaltszugriff ausschließt, zentrale Funktionen der Kollaborationsplattform also erheblich ein; die bloße Verfügbarkeit einer solchen Verschlüsselung belegt nicht, dass Kunden den Dienst mit unverändertem Funktionsumfang gegen Drittstaatenzugriffe absichern können. Hinzu kommt der Aufwand: Double Key Encryption erfordert zusätzliche beziehungsweise höherwertige Lizenzrechte (etwa Microsoft 365 E5 oder entsprechende Zusatzprodukte), wird nur in den Office-Desktop-Anwendungen unter Windows unterstützt und verlangt, dass der Kunde einen eigenen Schlüsseldienst betreibt — selbst oder über einen Dienstleister. Für ein kleines Unternehmen, eine Gemeinde oder einen Verein ist das weder finanziell noch personell ohne Weiteres umsetzbar; die wirksamste Schutzmaßnahme ist damit gerade für jene am schwersten erreichbar, die am wenigsten Verhandlungsmacht haben.

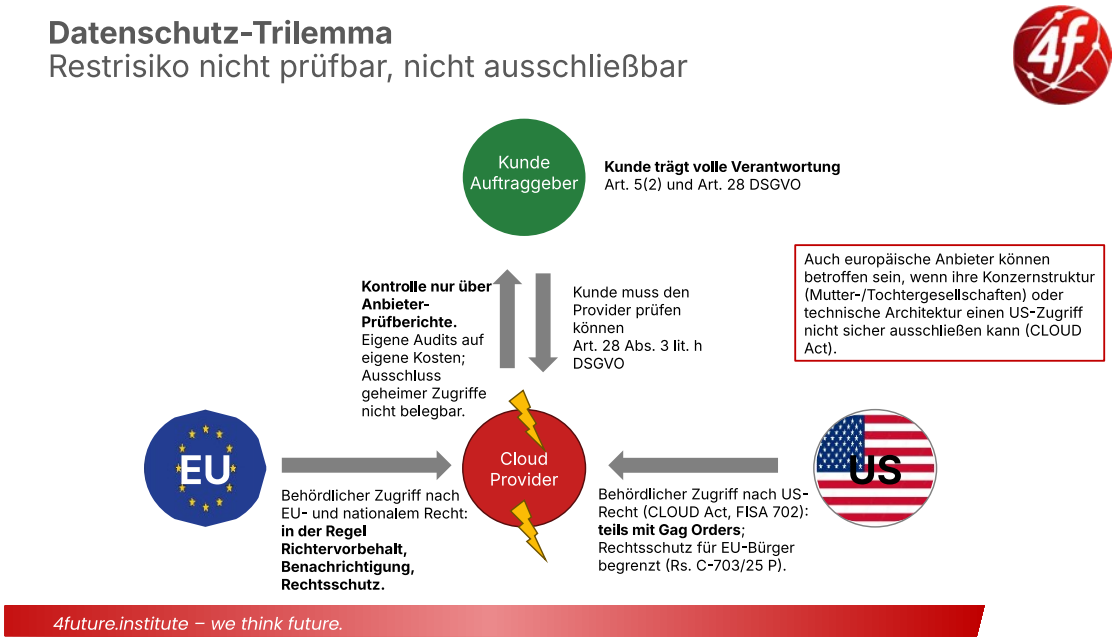
Der Europäische Datenschutzausschuss kommt für Cloud-Dienste, die zur Erfüllung ihrer Aufgabe Zugriff auf Daten im Klartext benötigen, zum selben Ergebnis: Er sieht sich nach dem Stand der Technik außerstande, eine wirksame technische Maßnahme zu benennen, die einen Zugriff durch Behörden eines Drittstaats mit unverhältnismäßigen Befugnissen verhindert (Empfehlungen 01/2020, Anwendungsfall 6). Für Dienste, die wie Microsoft 365 auf die Verarbeitung von Klartext durch den Anbieter ausgelegt sind, besteht damit ein Zielkonflikt: Je wirksamer eine Verschlüsselung den Anbieter ausschließt, desto weniger ist der Dienst nutzbar; die Schutzmaßnahme, die das beschriebene Risiko tatsächlich adressiert, hebt zentrale Funktionen des Dienstes auf. Ein Naturgesetz digitaler Zusammenarbeit ist das nicht: Es gibt Architekturen, die Ende-zu-Ende-verschlüsselte Zusammenarbeit mit Echtzeitbearbeitung im Browser ermöglichen, etwa CryptPad. Sie sind nicht in jeder Hinsicht gleichwertig und werfen eigene Vertrauensfragen auf, etwa nach dem ausgelieferten Programmcode, zeigen aber, dass Schutz vor dem Anbieter und Zusammenarbeit vereinbar sein können. Souveräne Alternativen sollten an genau dieser Frage gemessen werden. Ein pauschaler Verweis auf „geeignete technische und organisatorische Maßnahmen" ist deshalb keine tragfähige Begründung.

Jede Maßnahme ist an dem Risiko zu messen, das sie adressieren soll:

- **Speicherung in Europa:** Welche Zugriffs- und Kontrollmöglichkeiten bleiben außerhalb Europas bestehen?
- **Verschlüsselung:** Wer besitzt die Schlüssel und den Klartextzugriff — auch während der Verarbeitung?
- **Audit und Zertifizierung:** Welche Systeme, Zeiträume und Risiken wurden tatsächlich geprüft, und wer hat die Prüfung beauftragt?
- **Vertragliche Zusicherungen:** Welche Verpflichtungen sind auch im Konfliktfall durchsetzbar?
- **Datenexport:** Lassen sich Daten, Berechtigungen und Arbeitsabläufe bei einem Wechsel tatsächlich weiterverwenden (siehe Abschnitt 3.2.2)?
- **Ausstiegsplan:** Wurde der Wechsel unter realistischen Bedingungen erprobt und finanziell bewertet?

Wer die Schutzwirkung einer Maßnahme behauptet, muss ihre Voraussetzungen, ihre Reichweite und ihre Grenzen offenlegen.

Damit entsteht, was dieses Papier als Datenschutz-Trilemma bezeichnet: ein Spannungsverhältnis zwischen der vollen Rechenschaftspflicht des Verantwortlichen, seiner faktisch auf Berichte des Anbieters beschränkten Kontrolle über die Verarbeitung und konkurrierenden Rechtsansprüchen eines Drittstaats. Das Trilemma macht die Nutzung solcher Dienste nicht per se unzulässig. Es beschreibt ein Restrisiko, das der Verantwortliche weder vollständig prüfen noch vertraglich ausschließen kann. Für personenbezogene Daten mit hohem Schutzbedarf und für Tätigkeiten der öffentlichen Ordnung hält dieses Papier dieses Restrisiko für nicht hinnehmbar. Das ist eine politische Wertung, keine rechtliche Schlussfolgerung. Ebenso wichtig ist die Abgrenzung: Dass ein Zugriff nicht ausgeschlossen werden kann, ist kein Nachweis, dass er stattgefunden hat — es ist ein Befund über die Grenzen der Kontrolle.



Die Entwicklungen seit Erstpublikation dieses Papiers haben die beschriebene Rechtsunsicherheit weiter verschärft:

Im Januar 2025 entließ die Trump-Administration die demokratischen Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB) — der unabhängigen US-Aufsichtsbehörde, die die Einhaltung von Datenschutzverpflichtungen gegenüber der EU überwachen soll. Die Europäische Kommission hatte den PCLOB in ihrer Angemessenheitsentscheidung zum EU-US Data Privacy Framework (DPF) als zentrale Säule der institutionellen Absicherung 31 Mal explizit zitiert. Seitdem ist der PCLOB nicht beschlussfähig. Die Behörde besteht fort, kann aber keine Beschlüsse fassen; die in der Angemessenheitsentscheidung vorausgesetzte unabhängige Aufsicht ist damit erheblich geschwächt.

Das EU-US Data Privacy Framework selbst steht unter rechtlichem Druck: Eine erste gerichtliche Anfechtung wurde im September 2025 vom Gericht der Europäischen Union abgewiesen — das Rechtsmittel vor dem Europäischen Gerichtshof (Rs. C-703/25 P, eingelegt am 31. Oktober 2025) ist jedoch anhängig. Derselbe Gerichtshof hat die beiden Vorgängerrahmen (Safe Harbour 2015, Privacy Shield 2020) bereits für ungültig erklärt.

Hinzu kommt: Nach zwei kurzfristigen Verlängerungen im April 2026 ist FISA Section 702 — gemeinsam mit dem gesamten Titel VII des FISA — am 12. Juni 2026 ausgelaufen, erstmals seit 2008. Nach den Übergangsbestimmungen gelten bestehende Anordnungen, Genehmigungen und Weisungen bis zu ihrem Ablauf fort; Titel VII bleibt auf sie anwendbar, das FISA-Gericht behält seine Aufsichtsbefugnis, und die Anbieter bleiben zur Mitwirkung verpflichtet (Congressional Research Service, 2026). Die im März 2026 genehmigten Zertifizierungen gelten Berichten zufolge bis etwa März 2027. Danach unterliegt die bisher auf Section 702 gestützte Überwachung Titel I des FISA, der grundsätzlich Einzelanordnungen voraussetzt. Zum Zeitpunkt der Veröffentlichung hat der Kongress keine dauerhafte Neuregelung beschlossen. Die Bewertung des US-Schutzniveaus im Data Privacy Framework stützt sich auch auf den Rechtsrahmen von Section 702; wie die Kommission auf dessen Auslaufen oder eine Neuregelung reagiert, ist offen.

Diese Entwicklungen bestätigen die strukturelle Analyse dieses Papiers: Transatlantische Datentransfers beruhen auf einem rechtlich fragilen Fundament, das von politischen Entscheidungen in Washington abhängt — nicht von stabilen gesetzlichen Garantien.

Fazit: Europa verfügt derzeit nicht über rechtliche digitale Souveränität, solange kritische Daten durch Unternehmen verarbeitet werden, die fremden Rechtsordnungen unterliegen.

2.2 Technologischer Status: Abhängigkeit von nicht-europäischen Plattformen

Die europäische Verwaltung, Wirtschaft und Forschung stützen sich in wesentlichen Bereichen fast vollständig auf nicht-europäische digitale Plattformen, die größtenteils mit der europäischen Rechtssituation inkompatibel sind, und zu denen es kaum Alternativen gibt:

- **Cloud-Infrastruktur:** AWS, Microsoft Azure und Google Cloud halten rund 70 % des europäischen Cloud-Marktes; europäische Anbieter kommen zusammen auf rund 15 %, nach 29 % im Jahr 2017 (Synergy Research Group, 2025)
- **Kollaboration & Kommunikation:** Starke Abhängigkeit von Microsoft und Google. Eine Analyse von Compass Lexecon im Auftrag der Open Cloud Coalition, auf die sich eine Studie für das Europäische Parlament stützt, schätzt den gemeinsamen Anteil beider Anbieter am EU-Markt für Collaboration-Software auf bis zu 93 % (Datenbasis 2023). Die Werte sind modelliert: Sie beruhen auf kommerziellen Marktdaten, die anhand von Annahmen über Vertriebsnetzwerke angepasst wurden, fallen je nach Berechnungsszenario deutlich niedriger aus und weisen keinen gesondert ermittelten Anteil im öffentlichen Sektor aus
- **Softwareentwicklung:** GitHub (Microsoft) als global dominierende Plattform
- **Identitätsmanagement:** starke Abhängigkeit von Azure AD / Entra ID (Microsoft)
- **KI-Modelle & APIs:** überwiegend US-basierte Modelle und Trainingsinfrastrukturen

Diese Systeme sind proprietär, tief integriert und nur eingeschränkt portierbar. Dadurch entsteht zusätzlich ein struktureller **Vendor Lock-in**, der Wechsel oder Exit technisch und wirtschaftlich erheblich erschwert.

Erste Reaktionen der Industrie sind erkennbar — mit erheblichen Unterschieden in Substanz und Ernsthaftigkeit.

AWS hat im Januar 2026 die AWS European Sovereign Cloud allgemein verfügbar gemacht, eine von den übrigen AWS-Regionen physisch und logisch getrennte Cloud in der EU. Sie wird von einer neuen Muttergesellschaft und drei Tochtergesellschaften nach deutschem Recht betrieben, die von in der EU ansässigen Unionsbürgern geleitet werden; Betrieb und Support erfolgen durch in der EU ansässiges Personal. Die Gesellschaften bleiben jedoch Teil des Amazon-Konzerns. Der Ansatz geht damit über vertragliche Zusicherungen hinaus und adressiert operative Abhängigkeiten ernsthafter als bisherige Marktlösungen. Ob er Herausgabeanordnungen nach dem CLOUD Act ausschließt, hängt davon ab, ob die US-Muttergesellschaft rechtlich als im „Besitz, Gewahrsam oder in der Kontrolle“ (possession, custody, or control) der Daten gilt (18 U.S.C. § 2713) — eine Frage, die gerichtlich bislang nicht geklärt ist.

Microsoft hat im Februar 2025 die EU Data Boundary abgeschlossen: Kundendaten und pseudonymisierte personenbezogene Daten der zentralen Cloud-Dienste — darunter Microsoft 365 und die meisten Azure-Dienste — sowie Daten aus Supportfällen werden seither in der EU und der EFTA gespeichert und verarbeitet. Das ist eine umgesetzte Maßnahme zur Datenresidenz; die Rechtsstruktur ändert sie nicht, da die Dienste weiterhin von Gesellschaften erbracht werden, die der vollen Kontrolle der US-Muttergesellschaft unterliegen. Der Direktor für öffentliche und rechtliche Angelegenheiten von Microsoft Frankreich räumte im Juni 2025 unter Eid vor dem französischen Senat ein, dass eine Garantie gegen Datenzugriffe durch US-Behörden auch für in Frankreich gespeicherte Daten nicht gegeben werden kann.[1]

Für einen Vergleich sollten alle Angebote nach denselben Kriterien beurteilt werden: Eigentum und Kontrolle, operative Abhängigkeiten von der Konzernmutter, Möglichkeiten des Datenzugriffs, Verwaltung der kryptografischen Schlüssel, Abhängigkeit von Softwarelieferungen und die Fähigkeit zum Fortbetrieb bei Unterbrechung der Konzernbeziehung. Gemessen daran verbessern beide Ansätze Datenresidenz und operative Kontrolle in unterschiedlichem Umfang; keiner beseitigt die Zugehörigkeit zu einem Konzern, der dem US-Recht unterliegt.

[1] Sénat français, Commission des affaires économiques, Audition du 10 juin 2025 — senat.fr

Die praktische Relevanz dieser Exposition ist inzwischen sichtbar geworden. Nach US-Sanktionen gegen den Internationalen Strafgerichtshof (IStGH) im Februar 2025 wurde im Mai 2025 berichtet, dass der Chefankläger des Gerichtshofs den Zugang zu seinem bei Microsoft gehosteten E-Mail-Konto verloren habe; Microsoft hat diese Berichte bestritten. Im Oktober 2025 bestätigte der IStGH, Microsoft Office durch openDesk zu ersetzen, eine Open-Source-Suite des deutschen Zentrums für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS).

Diese Differenzierung ist analytisch relevant: Sie zeigt, dass der Markt beginnt, zwischen ernsthaften strukturellen Antworten und reinen Compliance-Narrativen zu unterscheiden — auch wenn keine der bisherigen Lösungen das Grundproblem vollständig löst.

Öffentliche Einrichtungen beginnen zu handeln. In Schleswig-Holstein waren bis Herbst 2025 rund 80 % der Arbeitsplätze der Landesverwaltung von Microsoft Office auf LibreOffice umgestellt. Das dänische Digitalisierungsministerium kündigte im Juni 2025 an, Microsoft 365 durch LibreOffice zu ersetzen. Das österreichische Bundesheer hat Microsoft Office auf rund 16.000 Arbeitsplätzen durch LibreOffice ersetzt. Im April 2026 wählte Frankreich Scaleway als Nachfolger von Microsoft Azure für den nationalen Health Data Hub; die Migration ist für Ende 2026 bis Anfang 2027 geplant. Im selben Monat vergab die Europäische Kommission einen Rahmenvertrag für souveräne Cloud-Dienste im Wert von bis zu 180 Millionen Euro über sechs Jahre an vier europäische Anbietergruppen, von denen eine S3NS umfasst, ein Joint Venture von Thales und Google Cloud. Diese Entwicklungen zeigen, dass Alternativen existieren — und dass die Bedeutung von „souverän“ in der Praxis umstritten bleibt.

Fazit: Europa verfügt nicht über technologische digitale Souveränität (wir können nicht über uns selbst entscheiden), da zentrale digitale Funktionen ohne mit Europäischem Recht kompatible Alternativen oder echte Kontrollmöglichkeiten betrieben werden.

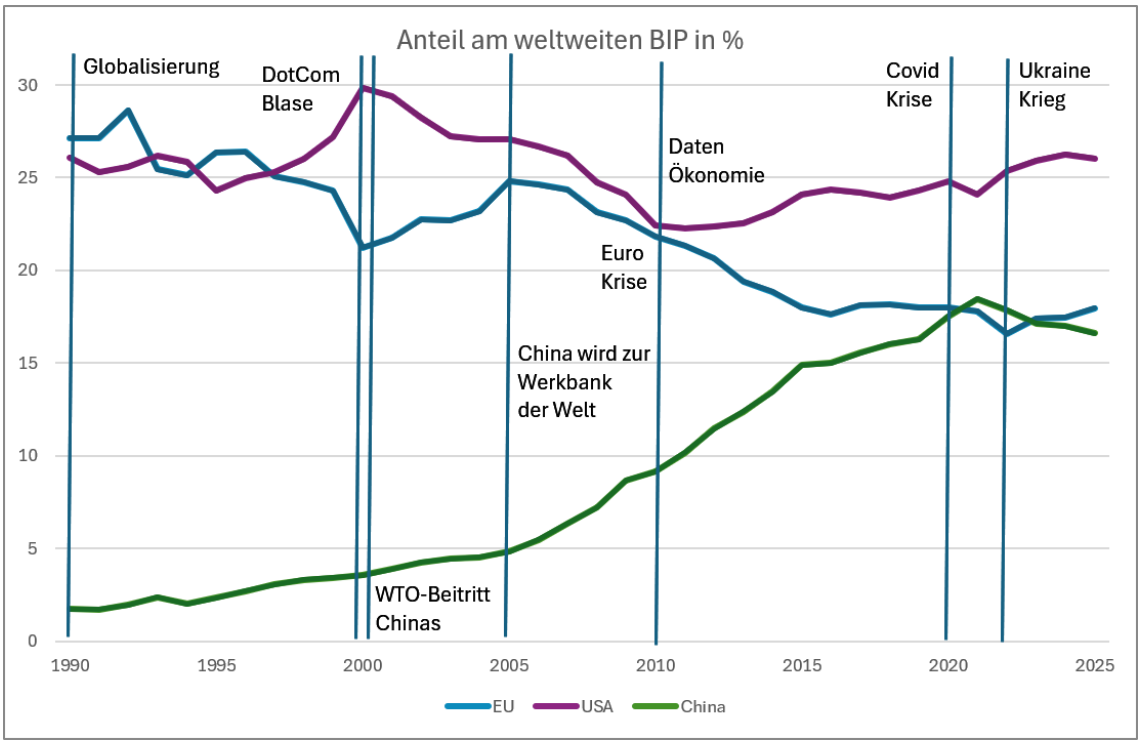
2.3 Ökonomischer Status: Wertschöpfungsverlust und strategische Verwundbarkeit

Die europäische Wirtschaft ist in zentralen Wertschöpfungsketten stark abhängig von Plattformen, deren Eigentümer, Rechtsrahmen und Entscheidungsstrukturen mit Europäischem Recht und Werten inkompatibel sind:

- Cloud-Dienste
- Kommunikations- und Kollaborationssysteme
- KI-Modelle und Trainingsinfrastrukturen
- Entwickler- und Deployment-Plattformen
- Identitäts- und Sicherheitsmechanismen

Diese Abhängigkeiten führen zu:

- **Wirtschaftlicher Abhängigkeit:** Wertschöpfung und Gewinne fließen überwiegend in Nicht-EU-Länder.
- **Strategischer Verwundbarkeit:** Plattformen können durch geopolitische Spannungen, Sanktionen oder politische Entscheidungen beeinflusst werden.
- **Eingeschränkter Verhandlungsmacht:** Preise, technische Standards und Vertragsbedingungen werden weitgehend von globalen Plattformbetreibern bestimmt.
- **Mögliche Wirtschaftsspionage:** Abfluss von wissenschaftlichen und industriellen Forschungsergebnissen



Anteil der EU-27, der USA und Chinas am weltweiten nominalen Bruttoinlandsprodukt (BIP), 1990–2025. 2025: IMF-Prognose. Quelle: International Monetary Fund (IMF), World Economic Outlook Database (Indikator NGDPD), 4future.institute.

Diese Entwicklungen haben Auswirkungen auf unsere Wirtschaft. Der Anteil der EU-27 am weltweiten nominalen BIP ist von rund 27 % im Jahr 1990 auf rund 18 % im Jahr 2025 gesunken; die EU liegt damit knapp vor China, das seinen Anteil im selben Zeitraum von unter 2 % auf knapp 17 % gesteigert hat. Die Grafik zeigt den Rahmen, nicht die Ursachen: Zum sinkenden Anteil tragen unter anderem Demografie, Wechselkurse, die Finanz- und Eurokrise und der Aufstieg Chinas zur Werkbank der Welt bei. Welchen Anteil digitale Abhängigkeit daran hat, lässt sich aus der Grafik nicht ableiten. Dieses Papier begründet ihre wirtschaftliche Bedeutung stattdessen mit konkreten Mechanismen: Wertschöpfung, die am Sitz der Anbieter anfällt, Lock-in und eingeschränkte Verhandlungsmacht (siehe unten und Abschnitt 3.3).

Unabhängig von den Ursachen dieser Kurve gilt: Europa hat in den letzten drei Jahrzehnten die digitale Infrastruktur, auf der seine Wirtschaft läuft, weitgehend ausgelagert. Was dabei abgeflossen ist, sind nicht nur Umsätze und Steuereinnahmen — es ist die Fähigkeit, digitale Wertschöpfung selbst zu gestalten.

Die USA haben diese Fähigkeit aufgebaut und verteidigt. China hat sie strategisch entwickelt. Europa hat sie bequem konsumiert.

Solange zentrale digitale Funktionen faktisch nicht ersetzbar sind, bleiben europäische Unternehmen und öffentliche Stellen den Preis-, Produkt- und Betriebsentscheidungen weniger Plattformanbieter ausgesetzt. Ein wachsender europäischer Digitalmarkt beseitigt diese Abhängigkeit nicht automatisch.

Fallbeispiel Kronstorf. Im April 2026 begann im oberösterreichischen Kronstorf auf rund 50 Hektar der Bau des ersten österreichischen Rechenzentrums von Google. Google nennt rund 100 direkte Arbeitsplätze; die Landesregierung bezeichnete das Projekt als größte Einzelinvestition in der Geschichte des Bundeslandes. Die öffentliche Debatte konzentrierte sich auf Strom, Wasser und Bodenverbrauch. Der Fall veranschaulicht drei unterschiedliche Dimensionen des in diesem Papier beschriebenen Problems.

Rechtsordnung: Der physische Standort eines Rechenzentrums ändert nichts an der Rechtsordnung, der sein Betreiber unterliegt. Eine Anlage in Österreich, die von einem US-Unternehmen betrieben wird, bleibt im Zugriffsbereich des CLOUD Act. Sie kann die Standortkriterien der in CADA vorgesehenen Basisstufe erfüllen, ohne den extraterritorialen Zugriff zu adressieren (Abschnitt 2.4).

Wertschöpfung: Rechenzentren sind hochautomatisiert. Der Bau schafft erhebliche, aber befristete Beschäftigung; der Betrieb erfordert vergleichsweise wenige dauerhafte Arbeitskräfte. Eine Studie der Joint Legislative Audit and Review Commission des US-Bundesstaates Virginia aus dem Jahr 2024 kam zum Ergebnis, dass Arbeitsplätze in Rechenzentren überwiegend befristete Bauarbeitsplätze sind; aktuelle britische Untersuchungen schätzen für neue Großanlagen nur 1,6 dauerhafte Arbeitsplätze pro Megawatt. Die Funktionen, die den größten Teil der Wertschöpfung erzeugen — Software- und Plattformentwicklung, Systemarchitektur, Produktentwicklung, geistiges Eigentum, Margen und die damit verbundene Steuerbasis — liegen dort, wo der Betreiber seinen Sitz und seine Entwicklungsorganisation hat. Bei einem US-Hyperscaler ist das überwiegend außerhalb Europas, bei einem europäischen Betreiber innerhalb Europas, wenn auch nicht zwingend im Standortstaat. Befürworter verweisen auf indirekte Beschäftigung, Effekte in der Zulieferkette und die Standortattraktivität; diese Effekte sind real, ändern aber nichts am Ort der zentralen wertschöpfenden Funktionen.

Energie: Laut Netz Oberösterreich könnte die geplante Erweiterung bis zu 4,4 TWh Strom pro Jahr verbrauchen — fast ein Drittel des gesamten oberösterreichischen Stromverbrauchs von 14 TWh im Jahr 2024. Dieser Bedarf entsteht in einer Zeit, in der sich Österreich und die Europäische Union zur Klimaneutralität verpflichtet haben. Selbst in Österreich mit seinem hohen Wasserkraftanteil setzen Gaskraftwerke Berichten zufolge rund zwei Drittel der Zeit den Großhandelspreis für Strom, und Österreichs Gas wird inzwischen überwiegend über Deutschland importiert, als norwegisches Pipelinegas und Flüssigerdgas (LNG). Zusätzlicher großer Bedarf, der nicht durch zusätzliche erneuerbare Erzeugung gedeckt wird, droht daher die Abhängigkeit von importierten fossilen Energieträgern zu vertiefen — und ersetzt eine strategische Abhängigkeit durch eine andere. Auf dem Papier erworbene Herkunftsnachweise ändern daran nichts, da sie bestehende erneuerbare Erzeugung umverteilen, statt neue hinzuzufügen (siehe Abschnitt 3.3.5).

Fazit: Europa verfügt nicht über ökonomische digitale Souveränität, da zentrale digitale Wertschöpfung nicht im eigenen Wirtschaftsraum entsteht und geopolitische Risiken nicht kontrollierbar sind. Das hat reale wirtschaftliche Auswirkungen.

2.4 Politische Entwicklungen: Der Cloud and AI Development Act (CADA)

Am 3. Juni 2026 legte die Europäische Kommission ihr Paket zur technologischen Souveränität vor. Kernstück ist der Vorschlag für eine Verordnung über einen Cloud and AI Development Act (CADA, COM(2026) 502 final, Verfahren 2026/0138(COD)). Titel IV des Vorschlags (Art. 16–31, Anhänge II und III) schafft erstmals im Unionsrecht einen Rahmen, der abgestufte Souveränitätsniveaus für Cloud-Dienste festlegt, die öffentlichen Stellen und Einrichtungen der Union bereitgestellt werden. CADA ist ein Vorschlag im ordentlichen Gesetzgebungsverfahren und unterliegt den Verhandlungen zwischen Europäischem Parlament und Rat.

Der Rahmen umfasst vier kumulative Stufen („Union assurance levels“), deren Kriterien in Anhang II festgelegt sind (Art. 16). Innerhalb eines Jahres nach Inkrafttreten und danach alle zwei Jahre müssen Mitgliedstaaten und Einrichtungen der Union Risikobewertungen durchführen, die jene Tätigkeiten des öffentlichen Sektors identifizieren, die zur Wahrung der öffentlichen Ordnung beitragen — in den von den Anhängen I und II der NIS-2-Richtlinie erfassten Sektoren sowie in den Bereichen nationale Sicherheit, innere Sicherheit, Außengrenzmanagement, Verteidigung, Justiz und Strafverfolgung —, und festlegen, ob für diese Stufe 2, 3 oder 4 angemessen ist (Art. 29 Abs. 1). Dabei sind unter anderem die Sensibilität der verarbeiteten Daten, das Risiko eines unrechtmäßigen Zugriffs durch Drittstaaten und das Risiko von Dienstunterbrechungen zu berücksichtigen (Art. 29 Abs. 2); hält die Kommission eine Zuordnung für unangemessen, kann sie per Durchführungsrechtsakt andere Stufen festlegen (Art. 29 Abs. 5). Die so identifizierten Tätigkeiten dürfen nur Dienste der Stufen 2, 3 oder 4 nutzen (Art. 30 Abs. 3); alle übrigen Tätigkeiten müssen mindestens auf Stufe 1 anerkannte Dienste verwenden (Art. 30 Abs. 2). Zusammengefasst:

Stufe 1: Der Anbieter ist in der Union niedergelassen; Infrastruktur, Vermögenswerte und Kundendaten — einschließlich Metadaten und Telemetriedaten — verbleiben in der Union, sofern die öffentliche Stelle nicht ausdrücklich anderes verlangt; der Dienst entspricht dem Stand der Technik der Cybersicherheit; der Einsatz von Unterauftragnehmern ist transparent (Anhang II Abschnitt 1.1 lit. a–f). Kontrolle durch einen Drittstaat ist zulässig. Ein solcher Anbieter muss gewährleisten, dass kein Recht und keine Praxis des Drittstaats ihn verpflichtet, Softwareschwachstellen an Behörden des Drittstaats zu melden, bevor sie als ausgenutzt bekannt sind (Anhang II Abschnitt 1.1 lit. g). Die Konformität wird durch Selbstbewertung und eine veröffentlichte EU-Konformitätserklärung nachgewiesen, mit der der Anbieter die Verantwortung für die Einhaltung übernimmt (Art. 19); Erklärungen von KMU werden in allen Mitgliedstaaten automatisch anerkannt (Art. 17 Abs. 3).

Stufe 2: Unabhängiges Audit durch Dritte (Art. 20). Anbieter und Unterauftragnehmer sind in der Union niedergelassen, Infrastruktur, Vermögenswerte und Personal befinden sich dort; erforderlich ist ein europäisches Cybersicherheitszertifikat der Vertrauenswürdigkeitsstufe „mittel" (bzw. bis zur Einführung eines solchen Schemas nationale Schemata); bei der Nutzung des Dienstes erzeugte Daten dürfen nicht zum Training von KI-Systemen verwendet werden, die von Einrichtungen aus Drittstaaten betrieben werden; der Support erfolgt ausschließlich innerhalb der Union; zudem gelten Maßnahmen für die Software-Lieferkette, darunter eine SBOM, Quellcode-Audits sicherheitsrelevanter Drittstaatenkomponenten und dokumentierte Migrationspläne (Anhang II Abschnitt 2.1). Kontrolle durch einen Drittstaat bleibt zulässig, sofern Maßnahmen gewährleisten, dass sie die Leistungserbringung nicht einschränkt, dass Zugriffe von Drittstaaten auf Kundendaten und Unterbrechungen der Dienstkontinuität verhindert werden und dass der Anbieter nicht zur Umsetzung von Sanktionen oder Embargos des Drittstaats verpflichtet werden kann (Anhang II Abschnitt 2.1 lit. g).

Stufe 3: Zusätzlich muss das Personal aus Unionsbürgerinnen und Unionsbürgern bestehen (mit nationaler Sicherheitsüberprüfung, soweit Verschlusssachen verarbeitet werden), und der Support muss von in der Union ansässigen Personen und von Dritten erbracht werden, die nicht der Kontrolle eines Drittstaats unterliegen (Anhang II Abschnitt 3.1 lit. d und h). Kontrolle durch einen Drittstaat ist grundsätzlich ausgeschlossen, kann aber zulässig sein, wenn die Kommission den Drittstaat per Durchführungsrechtsakt anerkannt hat (Anhang II Abschnitt 3.1 lit. g). Art. 18 legt dafür sechs kumulative Voraussetzungen fest, darunter einen Angemessenheitsbeschluss nach Art. 45 DSGVO, das Fehlen von Maßnahmen, die eine Kontrolle im Widerspruch zu den Regeln über den rechtmäßigen Zugang nach Art. 32 Data Act ermöglichen, sowie das Fehlen von Maßnahmen, die Dienstunterbrechungen oder die Befolgung von Sanktionen des Drittstaats erzwingen. (Anhang II Abschnitt 3.1 lit. g verweist auf einen Durchführungsrechtsakt „nach Artikel 19"; gemeint ist offensichtlich Art. 18.)

Stufe 4: Keine Kontrolle durch Drittstaaten, ohne Ausnahme; ein europäisches Cybersicherheitszertifikat der Vertrauenswürdigkeitsstufe „hoch"; sowie weitere Anforderungen an die Kontrolle über Softwarekomponenten (Anhang II Abschnitt 4).

Die Folgenabschätzung der Kommission (SWD(2026) 502) geht davon aus, dass rund 70 % der Anwendungsfälle im öffentlichen Sektor Stufe 1 erfordern, 20 % Stufe 2, 9 % Stufe 3 und 1 % Stufe 4. Diese Werte beruhen auf Gesprächen mit drei Behörden, die rund 200 öffentliche Auftraggeber vertreten, bei geschätzt 6.400 NIS-2-Einrichtungen; die Folgenabschätzung selbst bezeichnet sie als Annahme. Art. 30 Abs. 4 erlaubt öffentlichen Auftraggebern, ausnahmsweise und hinreichend begründet von der Beschaffung anerkannter Dienste abzusehen, wenn kein geeigneter anerkannter Dienst verfügbar ist, wenn eine vergleichbare Ausschreibung im Vorjahr keine geeigneten Angebote erbracht hat oder wenn die Anwendung der Anforderungen unverhältnismäßige Kosten verursachen würde; was unverhältnismäßig ist, definiert der Vorschlag nicht. Art. 32 verlangt bei der Beschaffung innovativer Cloud-Dienste und KI-Systeme nichtpreisliche Zuschlagskriterien, die den Beitrag des Bieters zu einem europäischen Cloud- und KI-Ökosystem bewerten; diese Kriterien müssen nachrangig sein und dürfen nicht ausschlaggebend sein, Erwägungsgrund 67 nennt eine Gewichtung von höchstens 15 von 120 Punkten.

Der abgestufte Ansatz ist grundsätzlich vertretbar: Nicht jede Anwendung im öffentlichen Sektor erfordert das höchste Schutzniveau, und Erwägungsgrund 52 beschreibt die Stufen als verhältnismäßigen Rahmen. Stufe 2 ist zudem anspruchsvoller, als ihre großzügige Behandlung der Drittstaatenkontrolle vermuten lässt, da sie einen nachweisbaren Schutz vor Datenzugriffen, Dienstunterbrechungen und der Durchsetzung von Sanktionen eines Drittstaats verlangt. Die Folgenabschätzung hält fest, dass ihre bevorzugte Option Anbietern mit Muttergesellschaft außerhalb der Union Stufe 3 nicht ermöglichen würde; der Gesetzestext sieht über die Anerkennung nach Art. 18 jedoch genau diese Möglichkeit vor.

2.4.1 Bewertung anhand der Anforderungen dieses Papiers

Einordnung in die bisherige Diskussion. Die bislang veröffentlichten Analysen zu CADA stammen überwiegend aus der anwaltlichen Beratungspraxis und richten sich an Anbieter und Unternehmen. Covington & Burling und Hogan Lovells beschreiben Aufbau und Stufen des Rahmens und benennen Unsicherheiten für Anbieter; Bird & Bird analysiert die Stufen als Bedingung des Marktzugangs und fragt, welche Anbietertypen welche Stufe erreichen können; Lawfare ordnet den Vorschlag aus transatlantischer Perspektive ein und weist darauf hin, dass die Voraussetzungen des Art. 18 US-Anbieter trotz Angemessenheitsbeschluss ausschließen könnten. Eurosmart, ein Verband der europäischen Digitalsicherheitsindustrie, fordert, Stufe 3 für Anbieter unter Drittstaatenkontrolle nicht zu öffnen. Die vorliegende Analyse unterscheidet sich davon in Perspektive und Maßstab: Sie bewertet den Vorschlag aus Sicht der öffentlichen Auftraggeber als Verantwortliche im Sinne der DSGVO — insbesondere kleinerer Stellen ohne eigene Prüfkapazität — und misst ihn an Kriterien, die vor seiner Veröffentlichung formuliert wurden. Mehrere der folgenden Befunde werden in keiner der genannten Analysen behandelt: das Fehlen einer Pflicht zur Verhinderung von Drittstaatenzugriffen auf Stufe 1; die Anknüpfung der Pflicht zu höheren Stufen an Sektor und Tätigkeit statt an die verarbeiteten Daten und die daraus folgende Unterschätzung horizontaler Plattformen; die undefinierte Kostenausnahme in Art. 30 Abs. 4; der Widerspruch zwischen Folgenabschätzung und Gesetzestext bei Stufe 3; die schmale empirische Basis der Verteilungsschätzung der Kommission; der fehlerhafte Verweis in Anhang II; sowie das Fehlen einer Zusätzlichkeitspflicht für Rechenzentren in Beschleunigungszonen. Diese Abgrenzung stützt sich auf die genannten Analysen und erhebt keinen Anspruch auf Vollständigkeit.

Gemessen an den in Abschnitt 3.1.2 formulierten Zertifizierungsanforderungen stellt CADA die richtige Frage. Fünf Aspekte verdienen im Gesetzgebungsverfahren jedoch kritische Aufmerksamkeit:

Die Basisstufe schützt nicht vor Drittstaatenzugriffen: Stufe 1 — die voraussichtlich den Großteil der Anwendungsfälle abdeckt — beruht auf Selbstbewertung und erlaubt Kontrolle durch Drittstaaten. Anders als Stufe 2 (Anhang II Abschnitt 2.1 lit. g Ziff. ii) enthalten ihre Kriterien keine Pflicht, Zugriffe von Drittstaaten auf Kundendaten zu verhindern; die Standortanforderungen können zudem auf Verlangen der öffentlichen Stelle entfallen. Für Anbieter, die dem CLOUD Act unterliegen, adressiert Stufe 1 daher das in Abschnitt 2.1 beschriebene Risiko extraterritorialer Zugriffe nicht — eine Einschränkung, die Microsoft vor dem französischen Senat selbst eingeräumt hat (siehe Abschnitt 2.2). Anerkannte Dienste der Stufe 1 tragen dennoch eine offizielle Bezeichnung innerhalb eines ausdrücklich als Souveränitätsrahmen bezeichneten Systems.

Die Pflicht zu höheren Stufen knüpft an Sektor und Tätigkeit an: Zwar verlangt Art. 29 Abs. 2 lit. a, die Sensibilität der Daten einschließlich personenbezogener Daten zu berücksichtigen; verpflichtend vorgeschrieben werden die Stufen 2 bis 4 jedoch nur für Tätigkeiten, die als Beitrag zur öffentlichen Ordnung in den in Art. 29 Abs. 1 lit. a genannten Sektoren und Bereichen identifiziert wurden. Für alle übrigen Tätigkeiten genügt Stufe 1 als Mindestanforderung, unabhängig davon, welche personenbezogenen Daten sie verarbeiten; öffentliche Stellen können höhere Stufen wählen, sind dazu aber nicht verpflichtet. In der organisatorischen Praxis bleiben personenbezogene und sensible Daten zudem nicht auf die Fachsysteme beschränkt, für die sie erhoben wurden: Sie werden in Tabellen exportiert, über Kollaborationsplattformen geteilt und als E-Mail-Anhänge versendet. Horizontale Büro-, Kollaborations-, E-Mail- und Identitätsplattformen verarbeiten daher typischerweise personenbezogene und häufig sensible Daten, unabhängig von der Einstufung der Fachanwendungen, aus denen diese Daten stammen.

Eine undefinierte Kostenausnahme: Art. 30 Abs. 4 lit. c erlaubt Abweichungen, wenn die Anforderungen unverhältnismäßige Kosten verursachen würden, ohne Verhältnismäßigkeit zu definieren. Da Wechselkosten mit der Tiefe bestehender Abhängigkeiten steigen, droht ein undefiniertes Kostenkriterium gerade jene Konstellationen zu begünstigen, deren Lock-in der Rahmen verringern soll.

Anerkennung von Drittstaaten per Durchführungsrechtsakt: Die Voraussetzungen des Art. 18 sind anspruchsvoll; insbesondere die Anforderung, dass ein Drittstaat über keine Maßnahmen verfügen darf, die Dienstunterbrechungen oder die Befolgung seiner Sanktionsregime erzwingen, dürfte mit dem geltenden US-Recht schwer vereinbar sein. Die Anerkennung erfolgt jedoch per Durchführungsrechtsakt und setzt einen Angemessenheitsbeschluss nach Art. 45 DSGVO voraus — einen Mechanismus, dessen derzeitige Anwendung auf die Vereinigten Staaten vor dem Europäischen Gerichtshof überprüft wird (Rs. C-703/25 P; siehe Abschnitt 2.1).

Keine Zusätzlichkeitspflicht für beschleunigte Rechenzentren: CADA will den Ausbau von Rechenzentren durch Beschleunigungszonen und verkürzte Genehmigungsverfahren vorantreiben (Art. 10–13). Bei der Ausweisung solcher Zonen müssen die Mitgliedstaaten Netzkapazität, saubere Erzeugung vor Ort und die Nutzung von Abwärme berücksichtigen (Art. 10 Abs. 1); die Nachhaltigkeitsanforderungen innerhalb der Zonen beschränken sich jedoch auf die Kennzahlen der Delegierten Verordnung (EU) 2024/1364 (Art. 11 Abs. 1). Eine Pflicht der Betreiber, zum Ausbau zusätzlicher erneuerbarer Erzeugung beizutragen, enthält der Vorschlag nicht. Beschleunigte Genehmigungen drohen damit die Nachfrage zu beschleunigen, ohne das entsprechende Angebot an erneuerbarem Strom zu beschleunigen (siehe Abschnitt 3.3.5).

Hinsichtlich der Wechselfähigkeit stützt sich der Vorschlag auf die Wechselbestimmungen des Data Act (Verordnung (EU) 2023/2854). Erfordert eine Risikobewertung den Wechsel zu einem anderen Dienst, muss die Migration innerhalb einer Übergangsfrist von höchstens zwölf Monaten erfolgen (Art. 29 Abs. 6), und die Risikobewertungen müssen prüfen, ob eine Multi-Vendor- oder Multi-Cloud-Strategie angemessen ist (Art. 29 Abs. 9). Die Stufen 2 und 3 verlangen zudem dokumentierte Migrationspläne für Softwarekomponenten aus Drittstaaten. Eine nachgewiesene, erprobte Ausstiegsfähigkeit der öffentlichen Stelle selbst macht der Vorschlag jedoch nicht zur allgemeinen Beschaffungsanforderung. Damit misst CADA, wie stark ein Dienst dem Einfluss von Drittstaaten ausgesetzt ist, nicht aber, ob er sich ersetzen lässt. Zur Souveränität gehört beides: die Kontrolle über den Anbieter und die Fähigkeit, ihn zu wechseln. Dass die Wechselbestimmungen des Data Act für komplexe Kollaborationsplattformen nicht ausreichen, weil ein Datenexport Arbeitsabläufe, Berechtigungen und organisatorischen Kontext nicht mitnimmt, zeigt das Begleitpapier zur Interoperabilität (siehe Abschnitt 3.2.2).

Kleine Auftraggeber: Quer zu diesen Punkten liegt eine Frage, die der Vorschlag kaum adressiert: ob kleinere öffentliche Stellen — Gemeinden, Schulen, kleinere Behörden — den Rahmen praktisch nutzen können. Die Risikobewertungen nach Art. 29 führen die Mitgliedstaaten durch; Auswahl, Beschaffung und Kontrolle der Dienste aber liegen bei der einzelnen Stelle. Sie muss die Unterschiede zwischen den Stufen beurteilen und Konformitätserklärungen oder Prüfberichte auswerten, deren Aussagekraft sie selbst kaum einschätzen kann; auf Stufe 1 liegt ihr nur die Selbstbewertung des Anbieters vor. Ob ein dokumentierter Ausstiegsplan im Ernstfall trägt, kann sie ohne eigene Erprobung nicht feststellen. Und die Kostenausnahme des Art. 30 Abs. 4 dürfte gerade dort in Anspruch genommen werden, wo Mittel und Fachpersonal fehlen. Ein Rahmen, dessen Anwendung eine Kontrollfähigkeit voraussetzt, die kleinen Auftraggebern fehlt, verlagert die Bewältigung struktureller Abhängigkeit auf jene, die sie am wenigsten leisten können.

Eine offizielle Souveränitätsbezeichnung ist daher nur in Verbindung mit zwei weiteren Angaben aussagekräftig: der betreffenden Stufe und der Frage, ob die Konformität auf Selbstbewertung oder auf einem unabhängigen Audit beruht. Beschaffungsentscheidungen, öffentliche Kommunikation und Marktangebote sollten beides ausweisen.

Fazit: CADA ist der erste ernsthafte Versuch, digitale Souveränität von politischer Rhetorik in überprüfbare rechtliche Kriterien zu übersetzen. Seine Wirksamkeit hängt vom Ausgang des Gesetzgebungsverfahrens ab — insbesondere von den Kriterien für Stufe 1, dem Anwendungsbereich der Risikobewertungen nach Art. 29, der Kostenausnahme in Art. 30 Abs. 4, den Voraussetzungen für die Anerkennung von Drittstaaten nach Art. 18 und den energiepolitischen Bedingungen für den beschleunigten Ausbau von Rechenzentren.

3 Handlungsoptionen zur Stärkung der digitalen Souveränität

Die Stärkung digitaler Souveränität erfordert einen **mehrschichtigen politischen Rahmen**, der rechtliche, technische, ökonomische und gesellschaftliche Maßnahmen integriert. Einzelmaßnahmen können Abhängigkeiten reduzieren, aber nur ein **kohärenter europäischer Strategierahmen** kann systemische Veränderungen bewirken.

Nachfolgend werden strategische Leitlinien sowie konkrete operative Maßnahmen vorgestellt.

3.1 Rechtlicher Rahmen

Klare Zuständigkeiten und Schutz vor extraterritorialen Zugriffen

Europäische digitale Souveränität benötigt einen Rechtsrahmen, der **Rechtsklarheit**, **Durchsetzbarkeit** und **Schutz vor fremden Rechtsordnungen** garantiert.

3.1.1 Anwendbares Recht klar definieren

- Einführung eines europäischen „Digital Jurisdiction Standard“, der festlegt: **Welche Rechtsordnung darf auf welche Daten zugreifen?**
- Verbot extraterritorialer Zugriffe auf europäische Datenräume durch Drittstaaten, sofern diese nicht EU-Recht entsprechen.

3.1.2 EU-weite Zertifizierung von Cloud- und KI-Diensten

Aufbau eines verbindlichen Zertifikats, das garantiert:

- Datenverarbeitung ausschließlich in Ländern, die mit dem europäischen Rechtsraum kompatibel sind (keine Aushebelung von Unionsrecht).
- keine Muttergesellschaft außerhalb des EU-Rechts (z. B. kein CLOUD-Act-Risiko)
- keine Tochtergesellschaften oder Niederlassungen außerhalb des EU-Rechts, die Zugriff auf europäische Daten haben
- Transparenzpflichten über staatliche Zugriffe

spezifisch für technische Plattformen.

CADA bietet für diese Anforderungen nun ein konkretes Gesetzgebungsinstrument (siehe Abschnitt 2.4). Für die Verhandlungen in Europäischem Parlament und Rat wären folgende Änderungen mit der Analyse dieses Papiers vereinbar:

- **Schutz und Prüfung auf Stufe 1:** Stufe 1 sollte eine Pflicht zur Verhinderung von Drittstaatenzugriffen auf Kundendaten enthalten und unabhängig geprüft werden — oder nicht als Teil eines Souveränitätsrahmens dargestellt werden.
- **Einstufung nach Daten:** Art. 29 sollte es ermöglichen, höhere Stufen auch auf Grundlage der verarbeiteten personenbezogenen und sensiblen Daten zuzuordnen, nicht nur für Tätigkeiten mit Bezug zur öffentlichen Ordnung; in der öffentlichen Verwaltung eingesetzte Büro-, Kollaborations-, E-Mail- und Identitätsplattformen sollten mindestens Stufe 2 erfordern.
- **Eine definierte Kostenausnahme:** Die Kostenausnahme in Art. 30 Abs. 4 lit. c sollte definiert, befristet, öffentlich begründet und an einen verbindlichen Migrationsplan geknüpft werden.
- **Anerkennung von Drittstaaten:** Die Anerkennung nach Art. 18 sollte auf gesetzlichen, unabhängig beaufsichtigten Schutzvorkehrungen im Drittstaat beruhen statt auf Angemessenheitsbeschlüssen, die sich auf exekutive Zusagen stützen; der Verweis in Anhang II Abschnitt 3.1 lit. g sollte berichtigt werden.
- **Ausstiegsfähigkeit als Kriterium:** Dokumentierte Datenportabilität, offene Formate und ein erprobter Ausstiegsplan sollten auf jeder Stufe verlangt werden; mittelfristig sollten die Stufen an eine europäische Interoperabilitätszertifizierung gekoppelt werden (siehe Abschnitt 3.2.2).
- **Transparenz:** Öffentliche Stellen sollten offenlegen, auf welcher Stufe jeder Cloud-Dienst beschafft wurde und worauf seine Anerkennung beruht (Selbstbewertung oder Audit).

Damit die Last nicht bei den kleinen Auftraggebern liegt, deren fehlende Kontrollmöglichkeiten dieses Papier beschreibt, sind darüber hinaus erforderlich:

- **Gemeinsam finanzierte Prüfungen:** Mitgliedstaaten oder Einrichtungen der Union sollten Prüfungen anerkannter Dienste gebündelt und im Namen aller öffentlichen Auftraggeber beauftragen, statt dass jede Stelle Prüfrechte einzeln verhandeln und bezahlen muss.

- **Fachliche Unterstützung:** Kompetenzstellen sollten Konformitätserklärungen und Prüfberichte für kleinere Auftraggeber auswerten und Musterbewertungen bereitstellen.
- **Gemeinsame Beschaffung:** Rahmenverträge auf nationaler oder europäischer Ebene sollten Prüf- und Ausstiegsrechte enthalten, die allen abrufberechtigten Stellen zugutekommen.
- **Verständliche Nachweise:** Für jeden anerkannten Dienst sollten öffentlich zugängliche Zusammenfassungen der Prüfergebnisse je Stufe verfügbar sein.
- **Erprobte Wechselmöglichkeiten:** Für die meistgenutzten Dienste sollten regelmäßige, öffentlich finanzierte Wechseltests durchgeführt und ihre Ergebnisse veröffentlicht werden.

3.1.3 Neuverhandlung transatlantischer Abkommen

Keine Abkommen ohne:

- Rechtsschutz für EU-Bürger
- Ausschluss geheimer Zugriffe (Gag Orders)
- technische und juristische Kontrollmechanismen

Die Dringlichkeit dieser Forderung hat sich seit Erstpublikation dieses Papiers konkret manifestiert: FISA Section 702 ist am 12. Juni 2026 nach zwei kurzfristigen Verlängerungen ohne dauerhafte Neuregelung ausgelaufen. Bestehende Genehmigungen gelten unter Aufsicht des FISA-Gerichts bis zu ihrem Ablauf fort; die künftige Rechtsgrundlage ist offen. Gleichzeitig ist der PCLOB, auf den sich das EU-US Data Privacy Framework als Aufsichtsinstitution stützt, seit Januar 2025 nicht beschlussfähig.

Diese Entwicklungen zeigen exemplarisch, warum bilaterale Abkommen, die auf Exekutivversprechen und nicht auf Gesetzesrecht basieren, strukturell unzuverlässig sind: Sie können durch eine neue Regierung mit einem einzigen Beschluss verändert oder ausgehöhlt werden — ohne europäische Mitsprache, ohne Vorankündigung.

Neuverhandlungen transatlantischer Abkommen müssen daher auf einer anderen Grundlage stattfinden: verbindliches Gesetzesrecht statt Exekutivorder, parlamentarische Kontrolle statt Behördenermessen, und echte Rechtsdurchsetzbarkeit für betroffene EU-Bürgerinnen und -Bürger.

3.1.4 Rechtsrahmen für kritische digitale Infrastruktur

- Definition, welche Systeme kritisch sind (z. B. Identitätsinfrastruktur, KI-Modelle, Behördenclouds).
- Verpflichtung dieser Systeme, ausschließlich in souveränen Infrastrukturen zu laufen

3.1.5 Globale Regulierung multinationaler Konzerne etablieren

Gleichzeitig braucht es internationale Regeln, um sicherzustellen, dass die Macht multinationaler Plattformen nicht die demokratischen Prozesse untergräbt. Staaten müssen gemeinsam Standards setzen, die:

- extraterritoriale Eingriffe begrenzen,
- Transparenz, Auditierbarkeit und Interoperabilität verpflichtend machen,
- monopolartige Strukturen verhindern,
- steuerliche Fairness sicherstellen.

Kein Staat – auch kein EU-Mitglied – kann dies allein umsetzen. Nur eine koordinierte internationale Regulierung kann die strukturelle Asymmetrie zwischen Staaten und Konzernen ausgleichen.

Ergebnis:
Ein Rechtsraum, der Kontrolle, Transparenz und Schutz vor fremden Rechtsansprüchen sicherstellt.

3.2 Technologischer Rahmen: Aufbau europäischer Kontrollfähigkeit

Rechtliche Vorgaben können nur wirken, wenn sie technisch umsetzbar sind.
Europa benötigt daher eine eigene, autonome digitale Funktionsfähigkeit, die sicherstellt, dass zentrale Dienste unabhängig von fremden Rechtsordnungen betrieben, überprüft und weiterentwickelt werden können. Technische Kontrollfähigkeit ist der Kern digitaler Souveränität – nicht Abschottung, sondern die Fähigkeit, digitale Infrastruktur selbst zu verstehen, zu betreiben und zu gestalten.

3.2.1 Aufbau einer europäischen Cloud- und KI-Infrastruktur

Europa benötigt eine föderierte, skalierbare und souveräne Cloud- und KI-Architektur, die zentrale digitale Funktionen unter EU-Recht betreibt.
Diese Infrastruktur muss folgende Eigenschaften erfüllen:

- **Betrieb ausschließlich nach europäischem Recht** – ohne extraterritoriale Zugriffsmöglichkeiten fremder Staaten.
- **Auditierbarkeit auf allen Ebenen** – Infrastruktur, Plattform, Software und KI-Modelle müssen technisch und rechtlich überprüfbar sein (Open Source oder offengelegte Komponenten).
- **Interoperabilität statt proprietäre Abhängigkeiten** – Dienste müssen austauschbar, portierbar und kombinierbar sein.

Bestehende Initiativen wie **GAIA-X** bieten hierfür einen Rahmen, adressieren jedoch nicht alle technischen und organisatorischen Anforderungen.
Sie sind ein Einstiegspunkt, aber **noch keine vollständige operative Lösung**.

3.2.2 Interoperabilität als verbindliche Grundlage

Interoperabilität ist die Voraussetzung für Wettbewerb, Wechselbarkeit und langfristige Kostentransparenz.
Sie muss daher als **verpflichtender Standard** in Europa verankert werden – insbesondere in Bereichen, in denen digitale Souveränität besonders relevant ist.

Dies umfasst:

- Kommunikation und Kollaboration: CalDAV, CardDAV, IMAP
- **Dokumente und Daten:** OpenDocument-Standards, offene Metadaten, offene API-Spezifikationen
- **Identität und Zugriffsmanagement:** OpenID Connect, European Digital Identity Wallet
- **Datenportabilität:** vollständig dokumentierte Exportformate und Schnittstellen

Interoperabilität schafft einen Markt, auf dem europäische Anbieter konkurrenzfähig sein können – und verhindert monopolartige Strukturen.

Das Begleitpapier „Digitale Souveränität braucht überprüfbare Interoperabilität“ (4future.institute, Juni 2026) vertieft diesen Abschnitt. Es zeigt, dass formal offene Standards allein nicht genügen: Dominante Plattformen setzen durch ihre Implementierungen faktische Referenzen, und Abhängigkeiten verlagern sich von Dateiformaten zu Arbeitsabläufen, Identitäten, Schnittstellen und KI-gestützten Wissenssystemen. Es schlägt deshalb eine europäische Interoperabilitätszertifizierung mit offenen Testverfahren und Referenzimplementierungen in drei Stufen vor — von der dokumentierten Unterstützung offener Standards über die volle Interoperabilität der Kernfunktionen bis zur verlustfreien Migration von Daten, Metadaten, Arbeitsabläufen und organisatorischem Kontext —, die schrittweise zur Voraussetzung öffentlicher Vergaben werden soll. Zudem empfiehlt es zu prüfen, ob Microsoft Office in allen Vertriebsformen als Torwächter im Sinne des Digital Markets Act zu benennen ist.

3.2.3 Europäische Identitäts- und Vertrauensdienste

Digitale Identität ist eine der zentralen Abhängigkeiten moderner digitaler Systeme.
Heute basieren große Teile europäischer Verwaltung, Wirtschaft und Bildungseinrichtungen auf proprietären US-Identitätsdiensten (z. B. Azure AD / Entra ID).

Daher wird eine europäische, öffentliche Identitäts- und Vertrauensinfrastruktur benötigt, die:

- als **Grundversorgung** fungiert – vergleichbar mit Energie- oder Kommunikationsnetzen,
- für Bürger, Unternehmen und Verwaltung gleichermaßen nutzbar ist,
- vollständig nach europäischen Rechtsnormen betrieben wird,
- föderiert, sicherheitszertifiziert und interoperabel ist,
- nicht von einzelnen Technologieanbietern abhängig ist.

Eine souveräne europäische Identitätsinfrastruktur ist notwendige Basis jeder digitalen Innovation – von KI über E-Government bis Cloud-Diensten.

3.2.4 Europäische Sicherheitsarchitektur

Sicherheitskritische digitale Infrastruktur muss in Europa überprüfbar, nachvollziehbar und frei von versteckten Zugriffsmechanismen sein.
Dazu gehören:

- **Förderung und Priorisierung europäischer Quelloffener-Lösungen** in Cybersecurity, Kryptographie, Netzwerkdiensten und Identitätsmanagement,
- Verpflichtende Offenlegung sicherheitsrelevanter Komponenten für Anbieter, die kritische Infrastruktur bedienen,
- **Gemeinsame europäische Standards** für Security Audits, Penetration Testing und Software Bills of Materials (SBOM),
- **Europäische Zertifizierung sicherheitskritischer Software** mit klaren Anforderungen an Transparenz, Protokolle und Architektur.

Sicherheit entsteht nicht durch Intransparenz, sondern durch Überprüfbarkeit und Kontrolle.

Ergebnis

Technische Souveränität entsteht nicht durch Abschottung, sondern durch Kontrollfähigkeit.
Eine europäische Cloud- und KI-Infrastruktur, interoperable offene Standards, eine souveräne Identitätsarchitektur und eine überprüfbare Sicherheitsbasis ermöglichen es Europa, digitale Systeme unabhängig zu betreiben und weiterzuentwickeln.
So entsteht ein stabiler digitaler Kern, der rechtliche, wirtschaftliche und sicherheitspolitische Maßnahmen erst wirksam macht.

3.3 Ökonomischer Rahmen: Marktmechanismen neu gestalten

Digitale Souveränität braucht einen wirtschaftlichen Rahmen, der Alternativen ermöglicht und Marktversagen korrigiert.

3.3.1 Strategische europäische Digitalinvestitionen / Innovation

Europäischer „Digital Sovereignty Fund“ zur Finanzierung von:

- KI-Modellen
- Cloud-Infrastruktur
- Hardwareproduktion

- quelloffenen und auditierbaren Kernkomponenten

Innovation entsteht nicht durch Abschottung, sondern durch Wettbewerb und Wahlfreiheit.

Ein funktionierender europäischer digitaler Markt braucht deshalb *mehr Anbieter*, *mehr Vielfalt* und *geringere Eintrittsbarrieren* – nicht ein „Europa baut alles selbst"-Szenario.

Monopolstrukturen – selbst, wenn sie europäisch wären – bremsen Innovation, begrenzen technologische Alternativen und verhindern die Entstehung neuer Geschäftsmodelle.

Offene Standards, interoperable Plattformen und transparente Rechtsräume schaffen hingegen einen Markt, auf dem Start-ups, mittelständische Unternehmen und europäische Entwickler*innen **neue, innovative Dienste** auf bestehenden Infrastrukturen aufbauen können.

Damit wird digitale Souveränität zu einem **Innovationsmotor**: Sie schafft einen fairen, offenen und wettbewerbsfähigen Binnenmarkt, in dem technologische Kreativität belohnt wird und nicht durch Lock-in-Effekte oder strukturelle Abhängigkeiten ausgebremst wird.

3.3.2 Reduktion wirtschaftlicher Abhängigkeiten

Unternehmen sollen befähigt werden, digitale Abhängigkeiten systematisch zu erkennen und zu bewerten – analog zu etablierten Verfahren im Risiko- und Lieferkettenmanagement.

Dadurch wird Transparenz geschaffen, ohne zusätzliche bürokratische Lasten aufzubauen.

3.3.3 Markt

Aktuell beziehen europäische Unternehmen und öffentliche Einrichtungen einen erheblichen Teil ihrer digitalen Infrastruktur von nicht-europäischen Plattformanbietern. Der Umsatz dieser Anbieter in Europa ist dabei nicht mit abfließender Wertschöpfung gleichzusetzen: Ein Teil verbleibt über lokale Beschäftigung, Partnerunternehmen und Steuern in Europa, und auch europäische Anbieter beziehen Hardware, Komponenten und Leistungen von außerhalb Europas. Die wertschöpfungsintensiven Funktionen — Entwicklung, geistiges Eigentum und Margen — liegen jedoch überwiegend am Sitz der Anbieter (vgl. Abschnitt 2.3).

Der Markt könnte vieles regeln – wenn wir tatsächlich einen funktionierenden Markt hätten. Doch in vielen digitalen Schlüsselbereichen existiert faktisch kein Markt mehr, sondern eine extreme **Konzentration auf wenige globale Plattformen**.

Digitale Souveränität bedeutet daher nicht, den Markt einzuschränken, sondern ihn überhaupt erst wieder herzustellen: durch **offene Standards, Wettbewerb, Wahlfreiheit** und **faire Rahmenbedingungen**, die Innovation ermöglichen, statt sie zu verhindern.

Maßnahmen zur Förderung von Interoperabilität, offenen Standards und europäischen Alternativen können hingegen zu einer Verlagerung von **Wertschöpfung nach Europa** führen: Rechenzentren, Softwareentwicklung, Forschung, Wartung und Betrieb können vor Ort erbracht werden und qualifizierte Arbeitsplätze, Steuereinnahmen und technologisches Know-how schaffen. Ein größerer Teil der Wertschöpfung bleibt so in Europa — vollständig allerdings nicht, da auch europäische Anbieter Hardware, Komponenten und Leistungen von außerhalb beziehen.

Förderprogramme für Migrationen, Investitionsanreize für interoperable Systeme und steuerliche Impulse für offene Technologien sind Subventionen. Gerechtfertigt sind sie dort, wo sie Übergangs- und Transformationskosten abfedern, Marktbarrieren senken und langfristig volkswirtschaftliche Erträge erwarten lassen; ihr Nutzen ist gegen ihre Kosten abzuwägen. Der öffentliche Aufwand ist zeitlich begrenzt, der erwartete strukturelle Nutzen wirkt dauerhaft: geringere Abhängigkeiten, höhere digitale Resilienz, eine breitere Wettbewerbsbasis und ein stabiler europäischer Technologiemarkt.

Fördermaßnahmen im Bereich digitaler Souveränität lassen daher nicht nur gesellschaftlichen und sicherheitspolitischen, sondern auch ökonomischen Nutzen erwarten; ob sie sich rechnen, ist für konkrete Programme anhand ihrer Kosten und Wirkungen zu belegen. Sie schaffen die Voraussetzungen dafür, dass Europa digitale Schlüsseltechnologien nicht ausschließlich konsumiert, sondern selbst entwickelt, betreibt und weiterentwickelt.

3.3.4 Europäische Beschaffungsreform

Die öffentliche Beschaffung ist eines der wirksamsten Instrumente, um digitale Souveränität zu stärken und faire Marktbedingungen herzustellen. Europäische Verwaltungen zählen zu den größten Nachfragern digitaler Dienste. Wenn sie systematisch auf offene Standards, transparente Rechtsräume und begrenzte Anbieterabhängigkeiten setzen, entsteht automatisch ein Marktumfeld, das Wettbewerb ermöglicht und Innovation fördert.

Konkret bedeutet dies:

(1) Priorisierung offener Standards gewährleistet, dass Systeme interoperabel bleiben, Daten portabel sind und Anbieterwechsel technisch möglich bleiben. Dies verhindert strukturelle Lock-in-Effekte und senkt langfristige Betriebskosten.

(2) Ausschluss extraterritorialer Rechtsrisiken stellt sicher, dass öffentliche Daten ausschließlich den Rechtsordnungen unterliegen, die demokratisch legitimiert und europäisch kontrollierbar sind. Dies ist insbesondere in kritischen Bereichen – Verwaltung, Polizei, Justiz, Gesundheit, Bildung – unverzichtbar.

(3) Begrenzung von Anbieterbindung durch klare Exit-Strategien, maximale Vertragslaufzeiten und technische Portabilitätsanforderungen stellt sicher, dass die öffentliche Hand nicht in einseitige Abhängigkeiten gerät, die teuer, riskant und schwer auflösbar sind.

(4) Vertragliche Ausstiegssicherungen machen Wahlfreiheit durchsetzbar: vollständiger Datenexport in offenen Formaten ohne Zusatzkosten, kundenseitig verwaltete Verschlüsselungsschlüssel, ein dokumentierter und erprobter Ausstiegsplan, Prüfrechte und maximale Vertragslaufzeiten. Ein Ausstieg, der nur auf dem Papier besteht, ist kein Ausstieg.

Das Ergebnis ist ein digitaler Beschaffungsmarkt, der Wahlfreiheit ermöglicht statt Oligopole zu verfestigen. Statt ungewollt monopolartige Strukturen zu stärken, fördert die öffentliche Hand so Wettbewerb, Innovation und europäische Alternativen. Dies reduziert langfristig Kosten, erhöht die Verhandlungsposition öffentlicher Stellen und stärkt die strukturelle Resilienz der europäischen digitalen Infrastruktur.

3.3.5 Energiepflichten für große Rechenzentren

Digitale Souveränität darf nicht auf Kosten energetischer Souveränität angestrebt werden. Das gilt unabhängig von der Herkunft des Betreibers: Auch europäische Betreiber müssen ihren Ressourcenbedarf und ihren Beitrag zur Versorgungssicherheit rechtfertigen. Große Rechenzentren sollten daher verpflichtet werden, zu den erneuerbaren Erzeugungskapazitäten beizutragen, die sie verbrauchen, statt auf bestehende Kapazitäten zurückzugreifen. Zwei Mitgliedstaaten bieten Referenzmodelle:

Irland: Nach der im Dezember 2025 von der Regulierungsbehörde Commission for Regulation of Utilities beschlossenen Netzanschlussregelung müssen neue Rechenzentren innerhalb von sechs Jahren nach Inbetriebnahme mindestens 80 % ihres jährlichen Strombedarfs aus zusätzlichen erneuerbaren Projekten decken, die in Irland erzeugen; während dieser Übergangszeit kann der Bedarf auch fossil gedeckt werden; bereits über bestehende Förderprogramme unterstützte Erzeugung wird nicht angerechnet. Die Regelung verlangt zudem steuerbare Erzeugung oder Speicher vor Ort oder in der Nähe — eine Anforderung, die in der Praxis mit Gaskraftwerken erfüllt werden kann und daher sorgfältig gestaltet werden sollte.

Deutschland: Das Energieeffizienzgesetz (EnEfG, § 11) verpflichtet Betreiber von Rechenzentren, ihren Stromverbrauch bilanziell durch Strom aus erneuerbaren Energien zu decken — zu 50 % ab 2024 und zu 100 % ab 2027 — und schreibt für neue Anlagen Mindestanteile wiederverwendeter Energie vor. Ein Gesetzentwurf sieht vor, die 100-%-Pflicht auf 2030 zu verschieben.

Österreich: Österreich befindet sich in einer strukturell anderen Lage als Irland. Mit rund 4,8 GW Pumpspeicherleistung — darunter die Kraftwerksgruppe Kaprun, die nach der Eröffnung von Limberg III (480 MW) im September 2025 auf 1.335 MW kommt — verfügt es über erhebliche Kapazitäten, um erneuerbaren Strom zu speichern und Flexibilität ohne neue Gaskraftwerke bereitzustellen. Pumpspeicher verschieben Strom jedoch zeitlich, statt ihn zu erzeugen, und die bestehenden Kapazitäten dienen bereits dem gesamten Verbundsystem. Eine österreichische Umsetzung des irischen Modells sollte daher eine Zusätzlichkeitspflicht für erneuerbare Erzeugung mit einem Beitrag zu zusätzlicher Speicherkapazität verbinden — etwa durch langfristige Verträge, die neue Pumpspeicherprojekte wie das geplante Kraftwerk Schaufelberg in Kaprun mitfinanzieren — statt steuerbarer fossiler Erzeugung vor Ort.

Solche Pflichten sind nicht nur eine Belastung für die Betreiber. Strom ist einer der größten Betriebskostenfaktoren eines Rechenzentrums; in Deutschland wird der Energieanteil an den Betriebskosten auf rund die Hälfte geschätzt. Erneuerbare sind die kostengünstigste Form neuer Stromerzeugung: Laut der Internationalen Agentur für Erneuerbare Energien (IRENA) war 2025 weltweit mehr als 90 % der neu errichteten erneuerbaren Großkapazität günstiger als die günstigste fossile Alternative. Nach dem Merit-Order-Prinzip bestimmt jedoch das teuerste zur Deckung der Nachfrage benötigte Kraftwerk den Großhandelspreis — häufig ein Gaskraftwerk —, sodass die niedrigen Kosten erneuerbarer Erzeugung nur teilweise bei den Verbrauchern ankommen. Langfristige Stromabnahmeverträge (PPAs) mit neuen erneuerbaren Anlagen und Speichern verschaffen Betreibern direkten Zugang zu diesen niedrigeren Erzeugungskosten und langfristige Preisstabilität. Speicher wiederum verschieben erneuerbare Überschüsse in Zeiten der Knappheit und verringern die Zahl der Stunden, in denen Gaskraftwerke den Preis setzen — zum Vorteil aller Verbraucher. Die Betreiber gehörten damit zu den Ersten, die von den zusätzlichen Kapazitäten profitieren, die sie mitfinanzieren. Zusätzlichkeit bringt die Interessen von Betreibern, Standortregionen und Energiewende in Einklang.

Daraus ergeben sich folgende Empfehlungen:

- **Zusätzlichkeit:** Ein wesentlicher Teil des jährlichen Strombedarfs großer Rechenzentren sollte durch neu errichtete, nicht geförderte erneuerbare Erzeugung im selben Land oder in derselben Gebotszone gedeckt werden, nicht allein durch Herkunftsnachweise.

- **Zeitlicher und regionaler Abgleich:** Erneuerbare Erzeugung sollte regional und, soweit möglich, stündlich statt jährlich mit dem Verbrauch abgeglichen werden. Eine Jahresbilanz erneuerbarer Erzeugung belegt keine durchgehende Versorgung; Erzeugung, Speicher, Netzkapazität und zeitliche Verfügbarkeit sind gemeinsam zu betrachten.
- **Speicher statt Gasturbinen:** Steuerbare Kapazität sollte durch zusätzliche Speicher und Nachfrageflexibilität bereitgestellt werden, nicht durch neue fossile Erzeugung.
- **Abwärmenutzung:** Mindestanteile wiederverwendeter Abwärme sollten Genehmigungsvoraussetzung sein, wo geeignete Wärmenetze bestehen oder geplant sind.
- **Beschleunigung mit Gegenleistung:** Beschleunigte Genehmigungen in CADA-Beschleunigungszonen sollten an Zusätzlichkeit und Abwärmenutzung geknüpft werden.
- **Transparenz:** Betreiber sollten Strom- und Wasserverbrauch, die Herkunft ihres Stroms und den Anteil zusätzlicher erneuerbarer Erzeugung offenlegen, als Grundlage für eine informierte Beteiligung der Öffentlichkeit (siehe Abschnitt 3.4.4).

3.4 Gesellschaftlicher Rahmen: Kompetenz, Transparenz und Teilhabe

Digitale Souveränität kann nur dann nachhaltig entstehen, wenn sie von der gesamten Gesellschaft getragen wird.

Ohne breite digitale Kompetenz, transparente Informationsgrundlagen und Beteiligungsmöglichkeiten bleibt digitale Souveränität ein Projekt für Expertinnen und Experten und entfaltet keine Wirkung im Alltag von Bürgerinnen, Unternehmen und Institutionen. Ein gesellschaftlicher Rahmen ist daher unverzichtbar, um digitale Unabhängigkeit langfristig zu verankern.

3.4.1 Bildung als Basis

Das europäische Bildungssystem ist noch immer stark auf **Reproduktion und Auswendiglernen** ausgerichtet. Für den souveränen Umgang mit digitalen Technologien jedoch braucht es vor allem **kritisches Denken, Problemlösungskompetenz** und die Fähigkeit, **Systeme zu hinterfragen**. Nur wer versteht, kann auch sicher, selbstbestimmt und verantwortungsvoll mit KI und digitalen Werkzeugen arbeiten.

Heute wirkt dieses Modell wie aus der Zeit gefallen: Digitale Technologien – und besonders KI – verlangen nicht die Wiederholung vorgefertigter Antworten, sondern **kritisches Denken, Problemlösung, Kontextverständnis und die Fähigkeit, gute Fragen zu stellen**.

Wer nur auswendig lernt, kann die Ergebnisse von KI nicht beurteilen.

Digitale Souveränität beginnt daher im Klassenzimmer: Wir brauchen ein Bildungssystem, das Neugier fördert, Widerspruch zulässt, eigenständiges Denken belohnt und Kinder ermutigt, ungewöhnliche Wege zu gehen.

Oder einfacher gesagt: Wir brauchen wieder **mehr Pippi Langstrumpf** – Menschen, die die Welt nicht nur so nehmen, wie sie ist, sondern sich zutrauen, sie anders zu denken.

Digitalbildung ist zusätzlich notwendig; daher sollten folgende Kompetenzfelder im Curriculum verankert werden:

- **Datenkompetenz**: Verständnis von Datenflüssen, Datenschutz, Einwilligung und Datenverarbeitung.
- **KI-Kompetenz**: Funktionsweise, Grenzen, Chancen und Risiken algorithmischer Systeme.
- **Cyber-Sicherheit**: Passwortkompetenz, Phishing-Erkennung und sicheres Verhalten im digitalen Alltag.
- **Funktionsweise digitaler Systeme**: Grundprinzipien von Netzwerken, Protokollen, Hardware und Software.

Ziel ist nicht technische Spezialisierung, sondern das Entstehen einer **digital mündigen Bevölkerung**, die informierte Entscheidungen treffen kann und nicht passiv abhängig von intransparenten Systemen bleibt.

Pädagogische Reformen allein reichen nicht aus. Schulen und Lehrkräfte benötigen dafür auch die notwendigen Ressourcen, Zeit und Unterstützung. Kritisches Denken, digitale Mündigkeit und KI-Kompetenz können nur entstehen, wenn das Bildungssystem sowohl strukturell als auch personell gestärkt wird.

3.4.2 Transparenz als Grundvoraussetzung für Vertrauen

Jede digitale Dienstleistung – privatwirtschaftlich oder staatlich – soll verpflichtet sein, in klar verständlicher Form offenzulegen:

- **wo** Daten verarbeitet werden,
- welcher Rechtsordnung sie unterliegen,
- welche technischen und organisatorischen Abhängigkeiten bestehen.

Diese Transparenz schafft Vertrauen, Vergleichbarkeit und informierte Entscheidungen. Sie ermöglicht es Bürgerinnen, Unternehmen und Behörden, digitale Angebote bewusst zu wählen – und stärkt damit den Markt für souveräne Systeme.

3.4.3 Europäischer Talent-, Forschungs- und Innovationsaufbau

Digitale Souveränität erfordert europäische Kompetenz in Schlüsseltechnologien. Dazu gehören:

- gezielte Förderung von unabhängiger öffentlicher Forschung in den Bereichen KI, Kryptographie, Cybersecurity, Cloud und Hardwareentwicklung (z.B. Chips, Server, Robotik, etc.),
- Aufbau europäischer Exzellenzzentren, die Hochschulen, Industrie und Start-ups vernetzen,
- Anreize für Technologie-Talente, die im Ausland tätig sind,
- verbesserte Rahmenbedingungen für europäische Tech-Gründungen, um Brain-Drain zu reduzieren.

Europa muss nicht nur digitale Technologien nutzen, sondern sie **selbst entwickeln und kontrollieren**, um global konkurrenzfähig zu bleiben.

3.4.4 Zivilgesellschaftliche Beteiligung an digitalen Großprojekten

Digitale Infrastruktur ist heute ebenso gesellschaftlich relevant wie Verkehr, Energie oder Umwelt. Daher sollten große digitale Vorhaben – ähnlich wie bei Umweltverträglichkeitsverfahren –:

- transparente öffentliche Beteiligungsprozesse durchlaufen,
- zivilgesellschaftliche und wissenschaftliche Expertise einbinden,
- Risiken, Alternativen und Auswirkungen offen darlegen.

Dies stärkt demokratische Legitimation, vermeidet Fehlentscheidungen und schafft Vertrauen in staatliche Digitalisierungsprozesse.

3.4.5 Globale Kooperation stärken

Europa sollte aktiv Partnerschaften mit Staaten aufbauen, die:

- rechtsstaatliche Prinzipien teilen,
- Datenschutz und Grundrechte achten,
- transparente und überprüfbare Governance-Strukturen haben.

Gemeinsam können interoperable technische Standards, sichere Datenräume und verantwortliche KI-Entwicklung gefördert werden. Kooperation schafft Skalierbarkeit, Innovationskraft und stabile globale Rahmenbedingungen.

Ergebnis

Digitale Souveränität wird zu einem gesamtgesellschaftlichen Projekt – nicht nur zu einem Regierungsprogramm.

Durch Bildung, Transparenz, Talentförderung und zivilgesellschaftliche Beteiligung entsteht eine breite Trägerbasis, die digitale Unabhängigkeit langfristig stabilisiert und demokratisch absichert.

4 Fazit

Digitale Souveränität ist keine technologische Option, sondern eine strategische Voraussetzung für die wirtschaftliche Stabilität, politische Handlungsfähigkeit und gesellschaftliche Resilienz Europas.

Die Analyse zeigt, dass Europa derzeit weder rechtlich, technologisch noch ökonomisch unabhängig agieren kann. Die Ursachen sind strukturelle Abhängigkeiten von Plattformen und Infrastrukturen, die außerhalb des europäischen Rechts- und Kontrollraums betrieben werden.

Eine Stärkung digitaler Souveränität gelingt nur durch einen systemischen Ansatz: durch einen klar definierten Rechtsrahmen, durch technologische Alternativen, durch wirtschaftliche Investitionen in europäische Wertschöpfung und durch eine Gesellschaft, die digitale Systeme versteht und aktiv mitgestaltet. Diese Maßnahmen verursachen Kosten, sind aber vor allem eine Investition in Europas Zukunftsfähigkeit. Sie schaffen lokale Wertschöpfung, reduzieren geopolitische Risiken und ermöglichen es Europa, seine fundamentalen Werte – Datenschutz, Demokratie und Wettbewerb – auch im digitalen Zeitalter zu sichern.

Digitale Souveränität, die auf Kosten energetischer Souveränität und der natürlichen Umwelt geht, ist keine Souveränität — sie ist eine verlagerte Abhängigkeit.

5 Call to Action

Europa steht an einem strategischen Wendepunkt. Digitale Souveränität ist keine abstrakte Zukunftsvision, sondern eine unmittelbare Voraussetzung für wirtschaftliche Stabilität, demokratische Kontrolle und gesellschaftliche Resilienz. Die kommenden fünf Jahre entscheiden darüber, ob Europa selbstbestimmt handelt – oder von externen Abhängigkeiten gesteuert wird.

Was jetzt notwendig ist, ist eine entschlossene europäische Agenda für digitale Souveränität:

- mit einem klaren durchsetzbaren rechtlichen Rahmen,
- mit einem Cloud and AI Development Act, dessen Souveränitätsbezeichnung unabhängig überprüft wird,
- mit überprüfbarer technologischer Infrastruktur,
- mit einem wettbewerbsfähigen **digitalen Binnenmarkt**,
- und mit einer **mündigen Gesellschaft**, die digitale Systeme versteht und souverän nutzt.

Digitale Souveränität hat ihren Preis — sie ist eine Investition in Europas Zukunftsfähigkeit und Innovationskraft.

Europa muss diese Chance entschlossen ergreifen

Jetzt!

I. Anhang: Über den Autor

Ing. Werner Illsinger, MBA, ist Gründer und Executive Director des 4future.institute. Er arbeitete 18 Jahre für Microsoft — von der Ära des Personal Computers bis in die Zeit der Cloud-Dominanz. Er hat erlebt, wie aus einem Unternehmen, das einst den PC demokratisiert hat, eine globale Plattforminfrastruktur wurde, die heute zentrale gesellschaftliche Funktionen kontrolliert — und zieht daraus Konsequenzen für Europa.

Ausgebildet als Nachrichtentechniker und Wirtschaftspsychologe verbindet er technisches Systemverständnis mit systemischer und gesellschaftlicher Perspektive. Dieses Papier ist kein Auftrag — es ist das Ergebnis einer wachsenden Überzeugung, dass Europa die strukturellen Bedingungen seiner digitalen Zukunft jetzt gestalten muss, solange das Fenster noch offen ist.

II. Anhang: Begriffsbestimmungen

Multi-Tenant-Cloud

Eine Architektur, in der viele Kunden dieselbe technische Infrastruktur (Server, Plattformen, Verwaltungsdienste) gemeinsam nutzen. Das ist effizient, verhindert aber, dass einzelne Kunden die zugrunde liegenden Systeme vollständig selbst prüfen oder isoliert betreiben können. Dadurch entstehen strukturelle Abhängigkeiten und eingeschränkte technische Kontrollmöglichkeiten.

Interoperabilität

Die Fähigkeit unterschiedlicher Systeme, Daten, Dokumente und Prozesse frei auszutauschen und zusammenzuarbeiten – ohne proprietäre Hürden oder Anbieterabhängigkeiten. Sie ist Voraussetzung für Portabilität, Wettbewerb und Innovationsfähigkeit.

Portabilität

Die Möglichkeit, Daten, Dokumente oder ganze Systeme ohne technische oder rechtliche Blockaden von einem Anbieter zum anderen zu übertragen. Portabilität verhindert Lock-in und stärkt den Wettbewerb.

Extraterritoriale Rechtswirkung

Wenn Gesetze eines Landes auch dann gelten, wenn die betreffenden Daten oder Personen in einem anderen Staat sind. Beispiel: Der US CLOUD Act verpflichtet US-Unternehmen, Daten herauszugeben – auch wenn diese in der EU gespeichert und EU-Recht unterliegen.

Vendor Lock-in

Eine Situation, in der Unternehmen oder Behörden faktisch nicht mehr zu einem anderen Anbieter wechseln können, weil proprietäre Schnittstellen, Formate oder Vertragsstrukturen einen Exit übermäßig teuer oder technisch schwierig machen.

Digitale Identität

Technische und organisatorische Mechanismen, mit denen Nutzer, Behörden oder Unternehmen ihre Identität nachweisen und digitale Dienste sicher nutzen können. Beispiele: EU Digital Identity Wallet, OpenID Connect.

Auditierbarkeit

Die Möglichkeit, technische Systeme unabhängig zu überprüfen – einschließlich Software, Architektur, Sicherheitsmechanismen und Datenverarbeitung. In Multi-Tenant-Clouds ist das nur eingeschränkt möglich.

SBOM (Software Bill of Materials)

Eine vollständige Liste aller Komponenten, Bibliotheken und Abhängigkeiten, aus denen eine Software besteht. SBOMs erhöhen Transparenz, Sicherheit und Nachvollziehbarkeit in Lieferketten.

III. Anhang: Quellen & Literatur

Rechtliche Grundlagen

- Datenschutz-Grundverordnung (DSGVO) – Regulation (EU) 2016/679
- CLOUD Act – Clarifying Lawful Overseas Use of Data Act, Public Law 115-141 (USA, 2018)
- FISA Section 702 – Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a
- EuGH – Schrems II (C-311/18) – Urteil des Europäischen Gerichtshofs vom 16. Juli 2020
- EU Charter of Fundamental Rights, Art. 7, 8 – Datenschutz, Privatsphäre

Marktdaten & wirtschaftliche Fakten

- Synergy Research Group (2024) – Global Cloud Market Share
- EU Industrial R&D Investment Scoreboard (2023/2024) – Investitionsschwerpunkte außerhalb Europas

Technische Grundlagen

- NIST SP 800-145 – The NIST Definition of Cloud Computing
- ENISA (2022, 2023) – Reports zu Cloud Security, Sovereignty & Multi-Tenant Architectures
- GAIA-X Architecture Documents (2023) – Federated Cloud Principles
- EU Cyber Resilience Act (2023/2024) – Anforderungen an sichere Software-Lieferketten
- SBOM Standards – NTIA / OASIS

Politische Debatten & Think-Tank-Analysen

- European Parliament Research Service (EPRS) – „Digital Sovereignty for Europe“
- Bertelsmann Stiftung – „Europas digitale Abhängigkeiten“
- Bruegel – „Open Strategic Autonomy and the Digital Transition“
- CERRE – „Cloud Competition & Regulation in Europe“

Bildung, Kompetenzen & Gesellschaft

- OECD – Future of Education & Skills 2030
- UNESCO – Digital Literacy Framework
- European Skills Agenda (2020–2025)
- World Economic Forum – Future of Jobs Reports (2020–2023)

Entwicklungen 2025–2026

- Europäische Kommission (2026) – Vorschlag für eine Verordnung über den Cloud and AI Development Act, COM(2026) 502 final, 3. Juni 2026
- Europäische Kommission (2026) – Anhänge zum CADA-Vorschlag, COM(2026) 502 final
- Europäische Kommission (2026) – Folgenabschätzung zu CADA, SWD(2026) 502
- Agence Europe (2026) – Commission wants European cloud providers to double market share to 30% (Bulletin 13883)
- Covington & Burling (2026) – The EU Cloud and AI Development Act in Depth
- Bird & Bird (2026) – Sovereignty as Market Access: What CADA's Assurance Levels Mean for Public-Sector IT Providers
- Hogan Lovells (2026) – The EU's Cloud and AI Development Act: Towards a Sovereignty-Focused Framework
- Eubelius (2026) – The Cloud and AI Development Act: Public Procurement as a Strategic Tool
- Lawfare (2026) – The EU Cloud and AI Development Act
- Congressional Research Service (2026) – The Impact of FISA Section 702's Repeal, LSB11444
- Amtsblatt der EU (2025) – Rechtsmittel in der Rechtssache C-703/25 P, Latombe/Kommission, C/2025/6610
- Synergy Research Group (2025) – European Cloud Providers' Local Market Share Holds Steady at 15%
- EJIL:Talk! (2025) – Why It Matters that the International Criminal Court Embraced Open-Source Software
- Heise (2025) – Schleswig-Holstein setzt auf Open Source und spart Millionen
- The Record (2025) – Denmark's Digital Ministry to Replace Microsoft with Open-Source Software
- Militär Aktuell (2026) – Warum das Bundesheer Microsoft Office durch LibreOffice ersetzt hat
- Plattform für Gesundheitsdaten (2026) – Pressemitteilung zur Migration zu Scaleway, 23. April 2026
- Der Standard (2026) – Die neue Schwerindustrie: Was hat Kronstorf vom KI-Boom?

- ORF (2026) – Großbaustelle von Google in Kronstorf
- MeinBezirk (2026) – Protest in Kronstorf gegen Großprojekt (Verbrauchsschätzung Netz Oberösterreich)
- Computing (2026) – UK Datacentre Jobs Claim Overstated by Three-Quarters, Says Research
- Nature Forward (2025) – Data Centers Are Said to Create Jobs (Zusammenfassung der JLARC-Studie, Virginia 2024)
- Der Standard (2025) – Merit-Order und Gas als preissetzende Technologie in Österreich
- ORF (2025) – Gasversorgung laut E-Control gesichert
- Commission for Regulation of Utilities (2025) – Decision on New Electricity Connection Policy for Data Centres
- Energieeffizienzgesetz (EnEfG), § 11 – Klimaneutrale Rechenzentren
- Gleiss Lutz (2026) – Gesetzentwurf zur Änderung des Energieeffizienzgesetzes
- Salzburg24 (2025) – Neues Verbund-Kraftwerk Limberg III in Kaprun fällt für Monate aus (Pumpspeicherleistung in Österreich)
- Leadersnet (2025) – Pumpspeicherkraftwerk Limberg III in Kaprun eröffnet
- Salzburg24 – Pläne für das Pumpspeicherkraftwerk Schaufelberg in Kaprun
- SolarQuarter (2026) – IRENA: Over 90% of New Renewable Power Added in 2025 Was Cheaper than Fossil Fuels
- KPMG – Drei Erfolgsfaktoren für die Zukunft deutscher Rechenzentren
- DatacenterDynamics (2026) – EU Commission Selects Four Cloud Providers under €180m Sovereign Cloud Tender
- Gineikyte-Kanclere, V. et al. (2025) – European Software and Cyber Dependencies, Studie für den ITRE-Ausschuss des Europäischen Parlaments, PE 778.576 (S. 49, Abb. 10)
- Microsoft – Microsoft Customer Agreement, Financial Services Amendment (Deutschland), Abschnitte 2–4 (Prüfungen durch Microsoft; Prüfrechte von Kunden und Aufsicht)
- Europäischer Datenschutzausschuss (2021) – Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools, Version 2.0 (Anwendungsfall 6)
- Microsoft – Double Key Encryption (Lizenz- und Systemanforderungen)
- Entrust (2024) – Microsoft Double Key Encryption and Entrust KeyControl, Integration Guide (unterstützte Anwendungen)

- CryptPad – Ende-zu-Ende-verschlüsselte Zusammenarbeit im Browser
- Microsoft – Double Key Encryption FAQ
- Microsoft – Enable co-authoring for files encrypted with sensitivity labels (Einschränkungen)
- Practical365 – Securing Copilot for Microsoft 365 (DKE-geschützte Inhalte)
- Illsinger, W. (2026) – Digitale Souveränität braucht überprüfbare Interoperabilität. Warum offene Standards alleine nicht ausreichen, 4future.institute, Version 1.1, 1. Juni 2026
- 4future.institute (2026) – Digitale Souveränität in Europa, Policy Brief, Version 2 vom 1. Juni 2026
- Eurosmart (2026) – Position Paper on the Cloud and AI Development Act (CADA)
- Hessischer Beauftragter für Datenschutz und Informationsfreiheit (2025) – Bericht zu Microsoft 365, Version 1.0, 15. November 2025
- Microsoft – Products and Services Data Protection Addendum (DPA), Abschnitt zur Prüfung der Einhaltung
- Microsoft – Microsoft Customer Agreement, Financial Services Amendment, Abschnitt 4 (Kosten von Kundenprüfungen: 4.000 US-Dollar pro Tag und Mitarbeiter)
- Microsoft – Get started with Microsoft Service Trust Portal (Prüfberichte, Geheimhaltungsvereinbarung)
- Microsoft (2025) – Microsoft completes landmark EU Data Boundary, 26. Februar 2025
- Amazon Web Services (2026) – AWS launches AWS European Sovereign Cloud, 15. Januar 2026
- 18 U.S.C. § 2713 – Required preservation and disclosure of communications and records (CLOUD Act)
- Europäischer Datenschutzausschuss (2021) – Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- International Monetary Fund – World Economic Outlook Database (Indikator NGDPD)

4future .institute
Wir denken Zukunft.

Gesellschaft. Wirtschaft. Technologie. Nachhaltigkeit.

Zukunft entsteht aus Balance und bewusster Gestaltung.

Das 4future Institute ist ein klar abgegrenzter Teilbereich der 4future business GmbH. Mehrheitseigentümerin ist die 4future.foundation.

Unabhängigkeit ist Voraussetzung unserer Arbeit — nicht ihr Ergebnis

4future.institute | Graben 17/10 | 1010 Wien | +43 1 31440-0 | hello@4future.institute