

PERSPEKTIVEN

Digitale Souveränität für Europa als Voraussetzung wirtschaftlicher Resilienz

Fähigkeiten entlang der gesamten digitalen Wertschöpfungskette in Europa stärken.

Digitale Souveränität ist entscheidend für die wirtschaftliche Wettbewerbsfähigkeit, sicherheitspolitische Handlungsfähigkeit und gesellschaftliche Resilienz. Europa steht dabei vor der Aufgabe, digitale Infrastrukturen, Datenhaltung und -bearbeitung sowie Anwendungen unter eigenen Regeln zu betreiben. Souveränität bedeutet nicht vollständige Unabhängigkeit, sondern Abhängigkeiten insbesondere bei Daten und Technologien aktiv und interessengeleitet zu gestalten und gezielt dort zu reduzieren, wo sie strategisch kritisch werden.

Dafür braucht es ein gemeinsames europäisches Verständnis, wie ein einheitlicher Handlungsrahmen für digitale Souveränität aussehen kann. Deutschland sollte im engen Schulterschluss mit Frankreich eine konsensfähige, substantielle Definition digitaler Souveränität erarbeiten. Maßnahmen nach dem Buy European Ansatz werden nicht ausreichen. Notwendig ist stattdessen ein gemeinsamer Maßnahmen- und Kriterienkatalog, der definiert, was souveräne digitale Infrastruktur ausmacht.



EXECUTIVE SUMMARY

Digitale Souveränität ist kein Zustand, sondern ein strategischer Prozess. Europa bleibt Teil globaler Technologieökosysteme, muss aber die Fähigkeiten stärken, zentrale digitale Infrastruktur, Daten und Anwendungen unter eigenen Regeln zu betreiben. Die derzeitige Debatte greift häufig zu kurz: Rechenzentren allein schaffen noch keine digitale Souveränität. Entscheidend ist das Zusammenspiel von Infrastruktur, Daten, Software, Energie, Kapital und Marktgestaltung entlang der gesamten digitalen Wertschöpfungskette. Es braucht einen gemeinsamen europäischen Ansatz, der digitale Souveränität als Frage strategischer Marktgestaltung versteht:

- **Öffentliche Beschaffung strategisch nutzen**
- **Investitionen in KI-, Cloud- und Chipinfrastruktur stärken**
- **Europäische Datenräume und offene Standards aufbauen**
- **Skalierung, Wettbewerb und digitale Wertschöpfung in Europa fördern**

Zentrale Hebel wurden im Rahmen eines umfassenden Technologiepaketes nun vorgestellt: der [Chips Act 2.0](#) setzt künftig auf Nachfrageimpulse und strategische Projekte; der [Cloud & AI Development Act \(CADA\)](#) soll einen einheitlichen EU-weiten Rahmen für Cloud- und KI-Souveränität schaffen; eine neue [Open-Source-Strategie](#) soll Alternativen in Cloud, KI und Cybersicherheit ausbauen. Ihre Wirkung entscheidet sich allerdings erst im laufenden Trilog.



Strukturelle Abhängigkeiten statt einzelner Defizite

Europas digitale Abhängigkeiten sind in zentralen Bereichen weiterhin ausgeprägt. Ein großer Teil des Cloud-Marktes wird von wenigen globalen Anbietern aus den USA oder China getragen. Zudem liegen bei leistungsfähigen KI-Chips und beim Training fortgeschrittener KI-Modelle erhebliche Teile der Wertschöpfungskette außerhalb Europas. Diese Entwicklung ist weniger Ergebnis einzelner Fehlentscheidungen als Ausdruck langfristiger Investitions-, Innovations- und Beschaffungsdynamiken.

Microsoft kündigte für 2025 Investitionen von rund 80 Milliarden US-Dollar in KI-fähige Rechenzentren an; das „Stargate“-Projekt sieht Infrastrukturinvestitionen von bis zu 500 Milliarden US-Dollar vor. Europa verfügt mit Frankreichs KI-Offensive, Mistral AI und einzelnen deutschen Initiativen über vielversprechende Ansätze, hat bislang jedoch kaum eigene Akteure hervorgebracht, die bei Kapitalausstattung und Skalierung mithalten können. Dabei ist ein Fokus auf Rechenzentren allein zu eng: Ohne Fortschritte bei Halbleitern, erneuerbarer Energie, KI-Ökosystemen und Datenverfügbarkeit bleibt ihr Beitrag zur Souveränität begrenzt.



Technologische Infrastruktur in Europa ausbauen

Digitale Souveränität erfordert eine integrierte Betrachtung der gesamten technologischen Wertschöpfungskette: von Chips über Energieversorgung bis hin zu datengetriebenen Anwendungen und

digitalen Zahlungssystemen. Europa sollte seine industriepolitischen Instrumente auf Segmente konzentrieren, in denen realistische Wettbewerbsvorteile bestehen – insbesondere Energie, industrielle Anwendungen, Automotive, Robotik und Edge-Computing. KMU müssen dabei besser eingebunden werden, etwa durch vereinfachten Zugang zu Chipentwicklung, Kompetenzzentren und europäische Kooperationsplattformen.

Der im Juni 2026 vorgelegte Chips Act 2.0 zieht Konsequenzen aus der Evaluation des ersten European Chips Act. Er verschiebt den Schwerpunkt spürbar: Statt pauschaler Marktanteilsziele rücken nachfrageseitige Maßnahmen, schnellere Industrialisierung von Pilotlinien und eine stärkere Ausrichtung auf strategische Anwendungsfelder in den Vordergrund – darunter Automotive, Energie, KI und Telekommunikation. Positiv ist zudem die Erweiterung des First-of-a-Kind-Rahmens auf Spezialmaterialien, fortgeschrittenes Packaging und fertigungsorientiertes Chip-Design, womit jene Wertschöpfungstiefe förderfähig wird, die Europas industrielle Stärke ausmacht. Diese Neuausrichtung entspricht einer WVG-Forderung: Europas Stärken in Mainstream-Halbleitern, Industrieanwendungen und Design gezielt zu stärken, anstatt im Technologiewettlauf bei Leading-Edge-Chips mitzubieten. Die industriepolitische Substanz des Vorschlags hängt allerdings am Ausgang der Verhandlungen zum mehrjährigen Finanzrahmen 2028–2034 – die Bundesregierung muss der Halbleiterindustrie dort die haushaltspolitische Priorität einräumen, die ihrer geopolitischen Bedeutung entspricht.

Der zeitgleich vorgelegte Cloud & AI Development Act (CADA) soll einen einheitlichen EU-weiten Rahmen zur Bewertung von Cloud- und KI-Souveränität einführen und Europa damit unabhängiger von einzelnen Anbietern machen, bei gleichzeitiger Marktoffenheit gegenüber Partnern. CADA führt ein vierstufiges Souveränitäts-Assurance-Framework ein, das Cloud-Dienste nach Datenschutz, operativer Autonomie und Jurisdiktionsrisiken klassifiziert. Öffentliche Auftraggeber werden verpflichtet, mindestens



Assurance-Level 1 einzuhalten; bei sicherheitsrelevanten Tätigkeiten gelten höhere Anforderungen. Die Bundesregierung muss sich im Triolog dafür einsetzen, dass das Assurance-Framework ambitioniert kalibriert wird, Interoperabilitätspflichten aus dem Data Act konsequent verknüpft werden und EU-Datenhaltungsanforderungen für kritische Bereiche verbindlich bleiben.

Ein weiterer Engpass liegt in der Energieinfrastruktur: Leistungsfähige Rechenzentren und KI-Anwendungen erfordern [erhebliche Strommen-gen](#). Europa kann klimafreundliche Energie-Infrastruktur als Wettbewerbsvorteil positionieren. Hierfür braucht es Tempo: Netzausbau und Genehmigungsverfahren sollten beschleunigt werden. Kommunale Akteure spielen dabei eine unterschätzte Rolle: Sie schaffen die Voraussetzungen für digitale Infrastruktur, von Energie- und Glasfaseranschlüssen bis zur Integration von Rechenzentrumsabwärme in lokale Wärmenetze. Auffällig ist, dass das angekündigte Data Centre Energy Efficiency Package fehlt, obwohl die Kommission verbindliche Effizienzstandards längst hätte vorlegen müssen. Stattdessen sieht die Roadmap lediglich eine Bedarfsabschätzung bis 2027 vor, was nicht ausreicht.

Souveränität im Zahlungsverkehr sichern

Unabhängige Bezahlssysteme sind nicht in jedem Mitgliedsstaat verfügbar und meist nicht paneuropäisch einsetzbar. Ein signifikanter Anteil der Wertschöpfung fließt jährlich an US-Anbieter. Initiativen wie Wero schaffen erste europäische Ansätze zur interoperablen Vernetzung nationaler Systeme, ergänzt durch den Digitalen Euro. Entscheidend sind Nutzerfreundlichkeit, Datenschutz und faire Wettbewerbsbedingungen, die europäischen Zahlungsanbietern Marktzugang auf Augenhöhe mit internationalen Akteuren ermöglichen. Die Ausgestaltung des Digitalen Euro sollte nicht zur Verdrängung erfolgreicher privater europäischer Angebote führen. In Verbindung mit der EUDI-Wallet eröffnet sich die Chance, A2A- (Account-to-Account) bzw. SEPA-Instant-Zahlungen in ein integriertes europäisches Ökosystem einzubetten, zur Stärkung technologischer Souveränität, Förderung von Wettbewerb

und Hebung von Skaleneffekten. Dazu gehört eine europäische Akzeptanzinfrastruktur, die private und öffentliche Zahlungslösungen gleichermaßen unterstützt und echte Wahlfreiheit ermöglicht. Auch die [FiDA-Verordnung](#) sollte souveränitätswahrend ausgestaltet werden: Open Finance kann Innovation fördern, darf aber keine neuen Wettbewerbsnachteile für europäische Finanzdienstleister schaffen.

Cybersicherheit ist wesentlicher Teil digitaler Souveränität

Mit der [NIS-2-Richtlinie](#), dem [Cyber Resilience Act \(CRA\)](#) und dem [Digital Operational Resilience Act \(DORA\)](#) hat die EU erstmals verbindliche Mindeststandards für die Resilienz digitaler Infrastruktur geschaffen. Unternehmen werden damit verpflichtet, Risiken systematisch zu analysieren und Abhängigkeiten entlang ihrer Lieferketten offenzulegen. Für viele Unternehmen bedeutet dies zunächst erhebliche Compliance-Anforderungen. Gleichzeitig entstehen jedoch erstmals einheitliche rechtliche Grundlagen, um digitale Resilienz gezielt aufzubauen. In jedem Fall sollten die regulatorischen Anforderungen möglichst bürokratiearm und gut aufeinander abgestimmt sein.

Ein gut ausgestalteter Cybersecurity Act 2 mit Trusted-Supplier-Ansatz, beschränkt auf kritische Infrastrukturen (Annex I NIS-2), wäre zentral, um strategische Abhängigkeiten sichtbar zu machen. Divergierende Meldepflichten, flächendeckende Dokumentationspflichten und komplexe Anforderungen binden knapp verfügbare Fachkräfte. Hier sollte risikobasiert entschlackt werden, ohne Standards zu senken. Ebenso wichtig ist der Aufbau interner Kompetenzen: Digitale Souveränität setzt voraus, dass Unternehmen und Behörden ihre Systeme nicht nur betreiben, sondern verstehen – und im Störfall eigenständig wiederherstellen können.



Daten, Recht und offene Systeme zusammen denken

Digitale Souveränität entsteht im Zusammenspiel von rechtlichen Rahmenbedingungen und technischer



Systemarchitektur. Europa verfügt mit der DSGVO über einen globalen Standard für den Schutz personenbezogener Daten. In der Praxis zeigt sich jedoch ein Spannungsfeld: Unternehmen können vorhandene Datenbestände häufig nicht rechtssicher für das Training von KI-Modellen nutzen, während der Rückgriff auf externe, oft außereuropäische Lösungen zunimmt, mit schleichender Verlagerung von Wertschöpfung und Innovationsfähigkeit. Regulatorik sollte Datenteilung besser ermöglichen, aber nicht erzwingen, und klare Rahmenbedingungen für lizenzbasierte Nutzungsvereinbarungen schaffen, ohne Geschäftsmodelle oder strategische Handlungsfähigkeit zu beeinträchtigen.

Für verantwortungsvolles KI-Training sind klare, praxistaugliche Regelungen Voraussetzung. Der [Digital-Omnibus zur KI-Verordnung](#) und die neue EU-Verordnung zu DSGVO-Durchsetzungsverfahren sind wichtige Schritte, adressieren jedoch nicht vollständig die Frage der rechtssicheren unternehmerischen Datennutzung. Ein zentraler Hebel wäre die Harmonisierung der Rechtsanwendung: Unterschiedliche DSGVO-Auslegungen in den Mitgliedstaaten erzeugen erhebliche Rechtsunsicherheit. Die Rolle des European Data Protection Board sollte gestärkt werden, um konsistente Anwendung und verbindliche Leitlinien für den KI-Kontext sicherzustellen.

Ermutigende Signale kommen aus dem laufenden Reformprozess: Der Digital-Omnibus diskutiert eine Neudefinition personenbezogener Daten, die pseudonymisierte Daten unter bestimmten Voraussetzungen herausnehmen würde; zudem soll die Verarbeitung besonderer Datenkategorien nach Art. 9 DSGVO zur Bias-Erkennung in KI-Systemen unter strengen Auflagen künftig erlaubt werden. Diese Entwicklungen sollten konsequent weiterverfolgt werden, mit dem Ziel, Datenschutz und datengetriebene Innovation stärker in Einklang zu bringen. Darüber hinaus sollte die Reform des Data Acts genutzt werden, um den Schutz von Geschäftsgeheimnissen und sensiblen Industriedaten zu stärken.

Open Source und offene Standards, statt Lock-In

Offene Standards, interoperable Systeme und gezielter Einsatz von Open-Source-Software sind technische Voraussetzungen für digitale Souveränität: Sie reduzieren Wechselkosten, verhindern Lock-in und ermöglichen Wettbewerb. Die [EU-Open-Source-Strategie](#) will europäische Alternativen in Cloud, KI und Cybersicherheit aufbauen, ein leistungsfähiges Ökosystem aus Unternehmen und Communities fördern und Open Source in öffentlichen Verwaltungen durch Leitlinien und Best Practices für die Beschaffung stärken. Ergänzend soll der Open Internet Stack Interoperabilität und offene Standards vorantreiben. CADA geht einen Schritt weiter und verpflichtet EU-Institutionen, Open-Source-Lösungen bei Neubeschaffungen stärker zu berücksichtigen und einen gemeinsamen Lösungskatalog aufzubauen. Das sind richtige Signale. Entscheidend wird sein, ob sie mit konkreten Zeitplänen und ausreichender Finanzierung unterlegt werden. Dabei sollte kein technologischer Ansatz grundsätzlich ausgeschlossen werden: Souveränität entsteht nicht durch die Wahl einer bestimmten Lizenzform, sondern durch Interoperabilität, Portabilität und die Vermeidung einseitiger Abhängigkeiten.

In Deutschland sollte eine Strategie für den öffentlichen Dienst verankert werden: Alle neuen IT-Vorhaben sollen, wo technisch und wirtschaftlich sinnvoll, auf Open-Source und offenen Standards basieren; bis 2027 ist eine Migration sicherheitskritischer Verwaltungssoftware erstrebenswert. Der [Interoperable Europe Act](#) setzt wichtige Impulse, bleibt aber in der Breite der Umsetzung bislang begrenzt.



Wettbewerb stärken und Marktgestaltung aktiv nutzen

Funktionierender Wettbewerb ist Voraussetzung für digitale Souveränität. Der europäische Binnenmarkt bietet hierfür grundsätzlich die richtigen Voraussetzungen, bleibt für digitale Geschäftsmodelle jedoch fragmentiert. Unterschiedliche



regulatorische Rahmenbedingungen, fehlende Skalierungsmöglichkeiten und begrenzter Zugang zu Wachstumskapital erschweren es europäischen Unternehmen, sich im globalen Wettbewerb zu behaupten. Zudem fehlt es an gemeinsamen europäischen Daten- und Innovationsökosystemen für grenzüberschreitende Zusammenarbeit. Gerade im industriellen Bereich liegt erhebliches Potenzial darin, anonymisierte Daten entlang gemeinsamer Standards zu nutzen – etwa zur Optimierung von Produktionsprozessen oder zum Training von KI-Modellen.

Instrumente wie der [Digital Markets Act \(DMA\)](#) und CADA adressieren zentrale strukturelle Probleme, insbesondere mit Blick auf faire Wettbewerbsbedingungen, Marktzugang und Interoperabilität. Entscheidend ist ihre konsequente und praxistaugliche Umsetzung. Die laufende DMA-Evaluation 2026 sollte genutzt werden, um Interoperabilitätsanforderungen zu schärfen und Sanktionsmechanismen wirksamer auszugestalten. Darüber hinaus muss Europa seine internationale Durchsetzungsfähigkeit stärken. Wirtschaftlicher Druck auf Unternehmen nimmt zu, insbesondere in geopolitisch sensiblen Technologiefeldern. Das Anti-Coercion Instrument (ACI) bietet erstmals ein Instrumentarium, um auf wirtschaftlichen Zwang zu reagieren – seine Wirkung hängt jedoch von der politischen Bereitschaft zur Anwendung ab.

Langfristig kommt es zudem auf die Weiterentwicklung des europäischen Binnenmarkts an. Einheitliche Rechtsformen für Unternehmen, etwa im Rahmen eines geplanten „28. Regimes“, könnten dazu beitragen, Skalierungshürden zu reduzieren und europäischen Tech-Unternehmen erstmals einen Heimatmarkt zu ermöglichen.



Öffentliche Beschaffung als zentraler Hebel

Der Staat ist einer der größten Nachfrager digitaler Produkte und Dienstleistungen in Deutschland. Bereits heute schließen Bund, Länder und öffentliche

Einrichtungen [milliardenschwere Verträge](#) für Software, Cloud- und IT-Infrastruktur ab, größtenteils mit außereuropäischen Anbietern. Damit entscheidet öffentliche Beschaffung maßgeblich darüber, welche Technologien sich durchsetzen und welche Anbieter skalieren können.

Trotz dieser Hebelwirkung wird öffentliche Beschaffung bislang unzureichend strategisch genutzt. Entscheidungen orientieren sich häufig an kurzfristigen Kosten, bestehenden Systemlandschaften oder operativen Zwängen, nicht systematisch an Kriterien digitaler Souveränität. Ein strategischer Ansatz würde Beschaffung gezielt als Instrument der Marktgestaltung einsetzen. Öffentliche Einrichtungen könnten als Ankerkunden für interoperable, sichere und europäisch anschlussfähige Lösungen fungieren, Nachfrage bündeln und Innovationsdynamik erzeugen.

Zugleich besteht erheblicher Koordinationsbedarf zwischen Bund, Ländern und Kommunen. Unterschiedliche Vergabestandards erschweren Skalierung und führen zu ineffizienten Parallelstrukturen. Deutschland sollte daher national wie europäisch auf eine stärkere Harmonisierung der Beschaffungsregeln hinwirken. Kommunale Unternehmen können dabei als Betreiber kritischer Infrastrukturen eine Schlüsselrolle spielen und durch Beschaffung, Datenhoheit und offene Standards digitale Souveränität unmittelbar stärken. Förderinstrumente und Beschaffung müssen stärker an Souveränitätszielen ausgerichtet und verzahnt werden, um Interoperabilität und Abbau von Abhängigkeiten gezielt zu unterstützen.

Digitale Souveränität entsteht nicht durch Abschottung, sondern durch bewusste Gestaltung technologischer Abhängigkeiten und Aufbau eigener Stärken. Entscheidend ist, Europa als attraktiven Standort für Innovation, Wertschöpfung und industrielle Anwendung zu stärken. Souveränität ist keine Frage der Herkunft von Technologien, sondern der eigenen Handlungsfähigkeit.



WAS TUN?

Vier Maßnahmen, die jetzt gebraucht werden, für eine digitale Souveränität, die auf europäische Stärken setzt, statt auf Abschottung:

1. Öffentliche Beschaffung strategisch ausrichten

Für IT-, Cloud- und KI-Beschaffungen sollten praxistaugliche Souveränitätskriterien entwickelt werden, etwa zu Interoperabilität, EU-Datenhaltung und rechtlichen Zugriffsmöglichkeiten. Europäische Technologieanbieter sollten bei Gleichwertigkeit bevorzugt berücksichtigt werden. Die Kriterien sollten einheitlich und verhältnismäßig ausgestaltet werden, damit sie Resilienz stärken, ohne Innovation und Wettbewerb einzuschränken. Statt nur der Preis, sollte auch der Resilienz-Wert der Produkte einbezogen werden.

2. Investitionslücke schließen: Europäischen KI- und Infrastrukturfonds aufsetzen

Während US-Technologiekonzerne Investitionen in dreistelliger Milliardenhöhe ankündigen, umfasst das gesamte EU-Forschungsprogramm Horizon Europe für sieben Jahre rund 95 Mrd. Euro. Das reicht nicht. Europa braucht einen gemeinsamen Hebel zur Mobilisierung von Kapital – ob öffentlich über einen KI-Infrastrukturfonds oder privat durch eine echte Kapitalmarktunion, einschließlich gezielter Förderung europäischer KI-Technologien.

3. Einheitliche Regeln für Datennutzung und KI-Training schaffen

Europa verfügt über große Datenbestände, nutzt diese bislang aber nur begrenzt. Rechtliche Unsicherheiten und uneinheitliche Regeln erschweren Datenaustausch und KI-Training. Entscheidend sind europäische Datenräume, die Datennutzung entlang gemeinsamer Standards ermöglichen – sicher, interoperabel und rechtsklar. Dazu gehört ein Nachschärfen des Data Acts zum Schutz von Geschäftsgeheimnissen und sensiblen Industriedaten. Neben einer harmonisierten Anwendung der DSGVO braucht es auch ihre innovationsfreundliche Weiterentwicklung, etwa durch rechtssichere Regelungen für pseudonymisierte Daten und das Training vertrauenswürdiger KI-Systeme.

4. Europäischen Digitalbinnenmarkt vertiefen und Skalierung erleichtern

Europäische Unternehmen scheitern häufig nicht an technologischer Kompetenz, sondern an fragmentierten Märkten, fehlendem Wachstumskapital und begrenzten Skalierungsmöglichkeiten. Einheitliche europäische Rechtsformen, bessere Bedingungen für Wachstumsfinanzierung und ein stärker integrierter Digitalbinnenmarkt sind entscheidend, damit digitale Wertschöpfung, Innovation und Investitionen stärker in Europa entstehen und bleiben. Dazu gehören auch interoperable Zahlungsinfrastrukturen (Wero, Digitaler Euro, SEPA-Instant, EUDI-Wallet) ebenso wie ein risikoorientierter und abgestimmter Umgang mit Cybersicherheitsanforderungen.

KOMMEN SIE JEDERZEIT GERN AUF UNS ZU

Aus der Wirtschaft, mit der Politik: In den Fachforen entwickeln die Mitglieder der Wirtschaftsvereinigung der Grünen Perspektiven und Impulse. Diese müssen nicht in jedem einzelnen Fall mit den Positionen jedes einzelnen Mitglieds übereinstimmen. [Mehr dazu hier.](#)

Die Wirtschaftsvereinigung der Grünen e.V.

Dorotheenstr. 3, 10117 Berlin

Hauptgeschäftsführung:

Martin Kaul, Katharina Krüger (stellv.)

Referent:innen Fachforum Innovation, Digitalisierung und Technologisierung:

Christoph Busch, Alisa Gropper, Lisa Reyman, Patrick Schuler