Digitale Souveränität

Positionsbestimmung und Handlungsempfehlungen für Deutschland und Europa



bitkom

Inhalt

Präambel 3

1 Definition – Was ist »Digitale Souveränität«? 4

Stand der Diskussion **4**

Die Perspektive in Deutschland und der Bundesregierung 4

Die Perspektive in der Europäischen Union 6

Begriffsbestimmung: Das verstehen wir unter Digitaler Souveränität **7**

Ausprägungen digitaler Souveränität **8**

2 Standortbestimmung: Wie digital souverän ist die deutsche Digitalwirtschaft? 9

Technologische Dependenz 9

Kriterienkataloge zur Messung digitaler Souveränität 11

3 Ziele: Welche Ziele sollten Deutschland und Europa verfolgen? 12

4 Maßnahmen: Aktionsplan Digitale Souveränität 13

Präambel

Seit der Veröffentlichung des ersten Bitkom-Positionspapiers zur Digitalen Souveränität im Jahr 2015 hat sich die Welt grundlegend verändert. Die geopolitische Lage ist heute von multiplen Krisen und globalen Handelskonflikten geprägt. Der kanadische Premierminister Mark Carney diagnostizierte beim Weltwirtschaftsforum in Davos im Januar 2026 den »Bruch der Weltordnung«. Die transatlantische Partnerschaft, die über Jahrzehnte das Fundament für Sicherheit, wirtschaftliche Integration und technologische Kooperation gebildet hat, kann heute nicht mehr als selbstverständlich gelten. Die Frage nach unserer digitalen Souveränität ist damit noch dringlicher für Staat, Wirtschaft und Gesellschaft geworden. Die von US-Vizepräsident J. D. Vance auf der Münchner Sicherheitskonferenz 2025 gehaltene Rede war ein Weckruf für Europa, die eigene digitale und wirtschaftliche Souveränität voranzutreiben. Der von Deutschland und Frankreich initiierte Gipfel zur europäischen digitalen Souveränität im November 2025 in Berlin setzte in diesem Kontext ein wichtiges politisches Signal für mehr digitale Unabhängigkeit in Europa.

Digitale Souveränität entscheidet über unsere wirtschaftliche Wettbewerbsfähigkeit, unsere politische Handlungsfähigkeit und letztlich über Wohlstand und Sicherheit. Digital souverän ist ein Land dann, wenn es eigene substanzielle Fähigkeiten in digitalen Schlüsseltechnologien besitzt und selbstbestimmt darüber entscheiden kann, aus welchen Ländern es digitale Technologien bezieht. Ein digital souveränes Land ist nicht einseitig abhängig. Gleichzeitig bedeutet digitale Souveränität nicht Autarkie, sondern technologische Selbstbestimmtheit. Deutschland verfügt bereits über eine starke technologische Basis: In zentralen Bereichen wie IT- und Cybersicherheit, industriellen Anwendungen wie dem Industrial Metaverse und dem Digitalen Zwilling sowie in der digitalen Gesundheitsversorgung und Medizintechnik nimmt es international eine führende Rolle ein. Auf diesen Stärken gilt es aufzubauen. Dafür braucht es gezielte Investitionen, bessere politische Rahmenbedingungen und einen Staat, der Innovationen fördert und als Ankerkunde neue Technologien in die Anwendung bringt. Ein innovationsfreundlicher Regulierungsrahmen ist ebenso entscheidend wie eine moderne Standortpolitik, die die gesamte digitale Wertschöpfungskette in den Blick nimmt – von Forschung und Gründung über Schlüsseltechnologien bis hin zu qualifizierten Fachkräften.

Deutschland und Europa haben technologisches Know-how, eine industrielle Basis und Innovationskraft. Entscheidend ist jetzt, diese Stärken konsequent in ein neues Souveränitätsmodell zu übersetzen: 1. Dort, wo wir eigene Technologien entwickeln können, müssen wir entschlossen investieren. 2. Wo wir bei kritischen Anwendungen auf internationale Technologien zurückgreifen, müssen diese sich an unsere Souveränitätsanforderungen anpassen. 3. Wo wir mit internationalen Tech-Unternehmen kooperieren, müssen bei sensiblen Anwendungen Kontrolle und Steuerungsfähigkeit in Deutschland und Europa verbleiben. Wenn Deutschland und Europa jetzt entschlossen handeln, können sie sich als starker Akteur in der Welt positionieren und so Wettbewerbsfähigkeit, Sicherheit und Wohlstand nachhaltig sichern. Digitale Souveränität ist kein optionales Ziel, sondern eine strategische Notwendigkeit. Dafür braucht es mehr Investitionen, klare regulatorische Anforderungen und klug gestaltete Partnerschaften. Aus diesem Dreiklang kann ein realistischer Weg zu mehr digitaler Souveränität entstehen.

1 Definition – Was ist »Digitale Souveränität«?

Stand der Diskussion

Die Diskussion über digitale Souveränität ist in Deutschland und Europa seit Jahren von Anpassungen, Umdeutungen und Abgrenzungen geprägt. Gerade vor dem Hintergrund technologischer und geopolitischer Entwicklungen gewinnt die Frage, was unter digitaler Souveränität konkret verstanden wird, zunehmend an Bedeutung. Die geopolitische Lage verdeutlicht dabei, dass technologische Abhängigkeit ein strategisches Risiko darstellt. Digitale Souveränität entwickelt sich somit zu einem zentralen strategischen Leitbegriff.

Die Perspektive in Deutschland und der Bundesregierung

Die Bundesregierung hat aus den geopolitischen Krisen Konsequenzen gezogen und strebt eine strategische Neuausrichtung an: »Unsere Digitalpolitik ist ausgerichtet auf Souveränität, Innovation und gesellschaftlichen Fortschritt. Digitalpolitik ist Machtpolitik. Wir wollen ein digital souveränes Deutschland.«[1] Ziel ist es, technologische Abhängigkeiten von Anbietern aus Drittstaaten zu verringern. Gleichzeitig soll die Entwicklung eigener Schlüsseltechnologien wie Künstliche Intelligenz, Halbleiter, Cloud und Cybersicherheit mit Initiativen der Hightech-Agenda gezielt gefördert werden.

Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) setzt auf den Ausbau einer leistungsfähigen deutschen Cloud-Infrastruktur. Im Fokus stehen offene Schnittstellen, europaweit anschlussfähige Standards sowie der verstärkte Einsatz von Open-Source-Technologien. Anbieter, die Anforderungen an Vertrauen und Sicherheit nicht erfüllen, sollen künftig konsequent ausgeschlossen werden können. Durch gebündelte IT-Aufträge soll der Staat gezielt als Ankerkunde der heimischen Digitalwirtschaft wirken. In diesem Kontext ist auch der »Deutschland-Stack« relevant, mit dem eine nationale souveräne Technologie-Plattform für Digitalvorhaben in Deutschland geschaffen wurde. Bis 2028 werden für Bund, Länder und Kommunen konkrete Angebote für eine souveräne, europäisch anschlussfähige und interoperable digitale Infrastruktur erarbeitet.

Aus sicherheitspolitischer Perspektive definiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Digitale Souveränität als die »Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.«[2] Zentral hierfür sei die Stärkung

[1] Koalitionsvertrag zwischen CDU, CSU und SPD, »Verantwortung für Deutschland. Koalitionsvertrag 2025–2029«, 2025.
[2] Bundesamt für Sicherheit in der Informationstechnik, ↗»Positionierung des BSI zu Digitaler Souveränität in Zeiten von Cyber Dominance«, 21. März 2025.

des europäischen Binnenmarkts und der eigenen Digitalindustrie sowie die Möglichkeit, internationale Produkte technisch so anzupassen und einzubetten, dass ein sicherer und selbstbestimmter Einsatz möglich wird.

Daneben betont die Bundesregierung, dass digitale Eigenständigkeit nur im Verbund mit europäischen Partnern möglich ist und daher strategische Allianzen geschlossen werden müssen. Gemeinsam mit Frankreich hat Deutschland am 18. November 2025 mit dem europäischen Gipfel zur digitalen Souveränität in Berlin ein deutliches Zeichen für mehr digitale Unabhängigkeit gesetzt. »Wir wollen mit dem heutigen Gipfel gemeinsam verdeutlichen, dass die digitale Souveränität Europas für Europa und für unsere gemeinsamen Werte zentral ist, aber auch für die Wettbewerbsfähigkeit unserer Wirtschaft, für unsere Sicherheit und für unsere Verteidigung«, so Bundeskanzler Friedrich Merz in der gemeinsamen Pressekonferenz mit dem französischen Präsident Emmanuel Macron. Der Gipfel soll der Startschuss für weitere konkrete Schritte sein, um die Kräfte in Europa zu bündeln und Abhängigkeiten abzubauen.

Das erste Ergebnis der im Nachgang des Gipfels gegründeten deutsch-französischen Taskforce ist die entwickelte gemeinsame Definition digitaler Souveränität, die Start der VivaTech im Juli 2026 in Paris von den beiden Ländern veröffentlicht wurde:

»Digitale Souveränität ist die Fähigkeit und Kapazität, digitale Technologien einschließlich Hardware auf unabhängige, selbstbestimmte und sichere Weise zu entwickeln, bereitzustellen, zu nutzen, anzupassen und zu kontrollieren, um die Fähigkeit der EU, eines Staates, einer Verwaltung oder einer privaten Organisation zu stärken, unabhängig zu handeln und die endgültige Entscheidungsgewalt über ihre Prozesse und Aktivitäten zu haben. Digitale Souveränität sollte konsequent auf die spezifische Risikokonstellation des jeweiligen Anwendungskontexts abgestimmt und auf technologisch und wirtschaftlich wettbewerbsfähige Lösungen ausgerichtet sein. Souveränitätsanforderungen sollten sich auf internationale Benchmarking-Vergleiche stützen und den Anspruch auf eine Führungsrolle verfolgen.

Die Stärkung der digitalen Souveränität zielt daher darauf ab, kritische Abhängigkeiten zu verringern und die aktive Entwicklung, Förderung und den Schutz von Schlüsseltechnologiebereichen sowie die Fähigkeit und Kapazität zur strategischen Entwicklung und zum Einsatz eigener Produkte und Innovationen zu fördern. Der Abbau von Abhängigkeiten darf nicht zu einer Isolation führen und sollte mit Partnerschaften mit vertrauenswürdigen internationalen Partnern einhergehen, sofern diese Partner unsere Anforderungen an die digitale Souveränität erfüllen. Diese Partnerschaften sind in diesem Zusammenhang ein entscheidendes Instrument. Es wird wichtig sein, sicherzustellen, dass europäische Akteure und Regierungen weiterhin Zugang zu modernsten digitalen Lösungen haben.«[3]

[3] Franco-German Joint paper on Digital Sovereignty vom 17. Juni 2026.

Die Perspektive in der Europäischen Union

Auf europäischer Ebene hat sich Digitale Souveränität als zentrales Leitmotiv etabliert. Die Europäische Kommission versteht darunter die Fähigkeit Europas, im digitalen Raum wettbewerbsfähig, resilient und eigenständig handlungsfähig zu sein, strategische Abhängigkeiten zu reduzieren und zentrale Technologien sowie Infrastrukturen unter europäischer Gestaltungshoheit weiterzuentwickeln. Im State of the Digital Decade 2025 spricht die Kommission ausdrücklich von dem Ziel einer »kompetitiven, souveränen, und resilienten EU«.[4] Im Juni 2026 hat die Kommission das Tech Sovereignty Package vorgestellt, das die europäische Wettbewerbsfähigkeit stärken und technologische Abhängigkeiten verringern soll. Auch institutionell hat das Thema deutlich an Gewicht gewonnen: Technologische Souveränität ist inzwischen ein eigenständiger Zuständigkeitsbereich der Exekutiv-Vizepräsidentin für Technologische Souveränität, Sicherheit und Demokratie, Henna Virkkunen.

Auch das Europäische Parlament treibt die Debatte aktiv voran. In seinem Initiativbericht zur technologischen Souveränität (2026) betont es die Notwendigkeit, Abhängigkeiten von einzelnen außereuropäischen Anbietern zu reduzieren und gleichzeitig Innovationsfähigkeit, Resilienz und Sicherheit zu stärken. Zugleich wird hervorgehoben, dass technologische Souveränität nicht als Abschottung zu verstehen ist, sondern Offenheit, Interoperabilität und Kooperation mit vertrauenswürdigen Partnern einschließt.[5]

Im Zuge dieser Entwicklungen hat sich mit der »EuroStack-Initiative« ein übergreifendes strategisches Leitbild herausgebildet. Ziel ist es, technologische Abhängigkeiten systematisch zu reduzieren und gleichzeitig ein leistungsfähiges, interoperables und wettbewerbsfähiges europäisches Digitalökosystem aufzubauen.

Gleichzeitig bestehen innerhalb der Europäischen Union unterschiedliche politische Akzentsetzungen in den Mitgliedsländern. Während Deutschland digitale Souveränität eher als offene, marktwirtschaftlich eingebettete Handlungsfähigkeit versteht, verfolgt Frankreich einen stärker auf Abschottung ausgerichteten Buy-European-Ansatz und eine aktivere Stärkung heimischer Wertschöpfung. Diese Unterschiede verdeutlichen, dass weiterhin um das richtige Gleichgewicht zwischen Offenheit, Resilienz, Wettbewerbsfähigkeit und staatlicher Steuerung gerungen wird – bei gleichzeitig wachsendem Konsens über die strategische Bedeutung digitaler Souveränität.

[4] European Commission, ↗»2025 State of the Digital Decade package«, 2025.
[5] European Parliament resolution on European technological sovereignty and digital infrastructure, ↗2025/2007(INI), 2026.

Begriffsbestimmung: Das verstehen wir unter Digitaler Souveränität

Unter dem Begriff »Souveränität« versteht man allgemein die Fähigkeit zu ausschließlicher Selbstbestimmung. Diese Selbstbestimmungsfähigkeit wird durch Eigenständigkeit und Unabhängigkeit gekennzeichnet. Sie grenzt sich einerseits von Fremdbestimmung und andererseits von Autarkie ab.

In einem Zustand der Fremdbestimmung verfügt ein Land über keine eigenen Fähigkeiten in Schlüsselbereichen. Es ist zudem nicht in der Lage, Fremdleistungen zuverlässig einzuschätzen und im Bedarfsfall zu veredeln oder zu härten. Es fehlt zudem die Fähigkeit, auf solider Basis zwischen alternativen Fremdleistungen zu unterscheiden und zu entscheiden.

Dem stehen autarke Systeme diametral gegenüber. Sie versorgen sich ausschließlich mit eigenen Angeboten aus eigenen Ressourcen. Dafür wird in Kauf genommen, dass autark erstellte Angebote weniger leistungsfähig und in der Herstellung aufwändiger sind als entsprechende Angebote Dritter. Autarke Staaten nehmen der Autarkie wegen bewusst Wohlfahrtsverluste und weitere Nachteile in Kauf. Autarkie ist in einer global vernetzten digitalen Welt weder zu erreichen noch anzustreben.

Souveräne Systeme hingegen sind zu selbstbestimmtem Handeln und Entscheiden befähigt, ohne ausschließlich auf eigene Ressourcen zurückzugreifen. »Digitale Souveränität« bezeichnet in diesem Sinne die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum. Digital souveräne Systeme verfügen bei digitalen Schlüsseltechnologien und -kompetenzen, entsprechenden Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau. Sie sind darüber hinaus in der Lage, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden, sie bewusst und verantwortungsvoll einzusetzen und sie im Bedarfsfall weiterzuentwickeln und zu veredeln. Nicht zuletzt sind souveräne Systeme in der Lage, ihr Funktionieren im Innern zu sichern und ihre Integrität nach außen zu schützen.

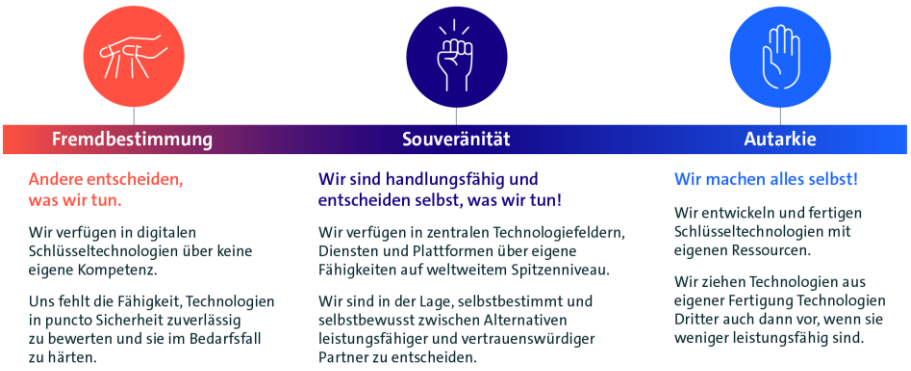


Abbildung 1: Fremdbestimmt, souverän, autark? – Die digitale Wirtschaft

Eine Grundvoraussetzung digitaler Souveränität ist in diesem Zusammenhang die Fähigkeit, die Geschäftsgeheimnisse der Unternehmen und Forschungseinrichtungen bestmöglich zu schützen. Gleiches gilt für die Privatsphäre der Bürgerinnen und Bürger.

Digital souveräne Systeme kennzeichnen sich dadurch, dass Wirtschaft, Wissenschaft und Gesellschaft Produkte, Dienstleistungen, Plattformen und Technologien unter Verwendung national und international zur Verfügung stehender Ressourcen entwickeln, zur Marktreife auf internationalem Spitzenniveau bringen bzw. dieses übertreffen und national und international vertreiben. Dabei unterstützt eine weltweite digitale Vernetzung.

Als digitale Schlüsseltechnologien und -kompetenzen begreifen wir

- Entwicklungs- und Produktionskompetenzen rund um IT-, Netzwerk- und Plattformsicherheit und
- Kompetenzen, digitale Technologien, Lösungen und Plattformen zu verstehen, zu prüfen, verantwortungsvoll einzusetzen und im Bedarfsfall so weitgehend zu veredeln und zu härten, dass sie den jeweils angestrebten Sicherheitsanforderungen entsprechen.

Ausprägungen digitaler Souveränität

Bei digitaler Souveränität ist zwischen zwei Ausprägungen zu unterscheiden:

- Anbietersouveränität: Selbstbestimmte Herstellung digitaler Technologien, Dienste und Plattformen.
- Anwendersouveränität: Selbstbestimmter Einsatz digitaler Technologien, Dienste und Plattformen Dritter.

Ein gesamtheitliches Konzept Digitaler Souveränität zielt also nicht nur auf die Befähigung zur selbstbestimmten Herstellung definierter digitaler Angebote ab. Ebenso ist es darauf ausgerichtet, digitale Technologien selbstbestimmt einsetzen zu können. Digitale Souveränität betrifft auch deshalb nicht nur die digitale Wirtschaft, sie betrifft in anderer Weise ebenso gewerbliche, private und öffentliche Anwender. Es geht bei Digitaler Souveränität also einerseits um digitale Leistungsfähigkeit von Unternehmen und andererseits um digitale Handlungsfähigkeit von Staat und Verbraucherinnen und Verbrauchern.

2 Standortbestimmung: Wie digital souverän ist die deutsche Digitalwirtschaft?

Technologische Dependenz

Digitale Souveränität ist einer der Faktoren für die Wettbewerbs- und Innovationsfähigkeit des Standorts Deutschland. Vertrauensvolle Beziehungen zu internationalen Partnern sind zwar ein zentraler Bestandteil einer starken Wirtschaft, doch dürfen sie nicht zu Fremdbestimmung führen. Wie im vorherigen Kapitel bereits beschrieben, geht es aber nicht um technologische Autarkie, sondern um das Ziel, in der digitalen Welt weiterhin selbstbestimmt Entscheidungen fällen zu können.

Die Bitkom-Studie von 2026 zeigt, wie abhängig die deutschen Unternehmen von digitalen Technologien und Services aus dem Ausland sind. Das Gesamtbild für die digitale Souveränität Deutschlands fällt schlecht aus: Die Ergebnisse zeigen eine wachsende Abhängigkeit der deutschen Wirtschaft vom Import ausländischer digitaler Technologien und Dienstleistungen: Die große Mehrheit der deutschen Unternehmen (96 Prozent) importiert digitale Technologien und Services aus dem Ausland. Besonders stark ist die Abhängigkeit bei Endgeräten wie Smartphones oder Laptops (94 Prozent), digitalen Bauteilen bzw. Hardware-Komponenten (79 Prozent) und Cloud-Computing-Diensten (73 Prozent). Auch Software (68 Prozent), Cybersicherheitsanwendungen (62 Prozent) und Künstliche Intelligenz (56 Prozent) werden von einer Mehrheit aus dem Ausland bezogen. Die wichtigsten Herkunftsländer für Digitalimporte sind die Vereinigten Staaten und China: 88 Prozent beziehen digitale Technologien und Leistungen aus den USA und 80 Prozent aus China. [6]

94%

der Unternehmen in Deutschland sehen Deutschland abhängig von digitalen Technologien und Leistungen aus dem Ausland.

↗Dataverse (2026)

Zudem wächst in der deutschen Wirtschaft die Sorge vor einer zu hohen Abhängigkeit von Cloud-Diensten aus dem Ausland, wie der Cloud-Report 2026 des Bitkom zeigt.[7] Fast zwei Drittel (62 Prozent) der Unternehmen in Deutschland würden ohne Cloud-Dienste stillstehen. Zugleich halten mehr als drei Viertel (85 Prozent) Deutschland für zu abhängig von US-Cloud-Anbietern, 80 Prozent wünschen sich große Cloud-Anbieter, sogenannte Hyperscaler, aus Deutschland oder Europa, die es mit den außereuropäischen Marktführern aufnehmen können. Und jedes zweite Unternehmen (50 Prozent), das Cloud-Computing nutzt, sieht sich aufgrund der Politik der neuen US-Regierung gezwungen, die eigene Cloud-Strategie zu überdenken.

Auch im Bereich Künstliche Intelligenz wächst die Sorge vor technologischen Abhängigkeiten. Laut aktuellen Bitkom-Daten[8] sind 72 Prozent der Deutschen der Meinung, dass Deutschland im Bereich KI zu abhängig von den USA ist. Gleichzeitig

[6] Bitkom e. V., »Digitale Souveränität – wie beenden wir die Abhängigkeiten?«, 2026.
[7] Bitkom e. V., ↗Cloud Report 2026.
[8] Bitkom Research, ↗Dataverse: Bevölkerung zu Künstlicher Intelligenz, 2026.

würden 67 Prozent bevorzugt eine KI aus Deutschland nutzen und 65 Prozent sprechen sich dafür aus, dass die EU eigene KI-Systeme entwickelt.

Dieses Lagebild spiegelt sich auch im Digital Dependence Index (DDI) der Universität Bonn wider, der die Dependenzgrade von 23 untersuchten Staaten in unterschiedlichen Technologiebereichen misst. Verglichen wird das Ausmaß der Abhängigkeiten beim Handel mit digitalen Gütern und Dienstleistungen, im Bereich der Informations- und Kommunikationsinfrastrukturen und hinsichtlich der geistigen Eigentumsrechte für digitale Technologien.[9] Deutschland wurde eine »hohe Vulnerabilität« attestiert, was auf eine sehr niedrige digitale Autonomie und eine dominante Rolle ausländischer Technologien hinweist.

Das Vertrauensniveau der deutschen Wirtschaft in internationale Partner variiert stark, wie die Bitkom-Studie zeigt: Das größte Vertrauen haben Unternehmen gegenüber anderen Mitgliedstaaten in der EU (97 Prozent). An zweiter Stelle folgt Japan, dem 73 Prozent der Unternehmen eher oder sehr großes Vertrauen entgegenbringen. Mit 60 Prozent und also deutlichem Abstand hinter Japan findet sich Großbritannien auf Rang 3. In die USA hat jedes zweite Unternehmen (51 Prozent) eher oder sehr großes Vertrauen. Noch mehr Skepsis herrscht gegenüber China: Nur jedes vierte deutsche Unternehmen (26 Prozent) hat sehr oder eher großes Vertrauen. Das Vertrauen der deutschen Wirtschaft für Russland ist praktisch an einem Nullpunkt angekommen. 97 Prozent der Unternehmen geben an, »gar kein Vertrauen« in Russland zu haben.

Die hohe Abhängigkeit bei Digitalimporten hat einen Großteil der Unternehmen bereits zu Gegenmaßnahmen veranlasst. 44 Prozent der Unternehmen, die digitale Technologien und Leistungen aus dem Ausland beziehen, setzen verstärkt auf Anbieter aus Deutschland und Europa. 41 Prozent halten größere Vorräte bei wichtigen Bauteilen und Komponenten vor, um mögliche Lieferengpässe abzufedern. 40 Prozent bereiten sich darauf vor, bei Bedarf wichtige Anbieter und Systeme auswechseln zu können. 32 Prozent bauen eigenes technisches Know-how auf, 31 Prozent beziehen wichtige Produkte, Komponenten oder Services von mehreren Lieferanten.[10] Den Ernst der Lage haben die Menschen in Deutschland verstanden: 99 Prozent der Bundesbürgerinnen und Bundesbürger finden es wichtig, dass Deutschland bei digitalen Technologien insgesamt unabhängiger wird.[11] Zudem fordert eine große Mehrheit von 79 Prozent ein staatliches Eingreifen, wenn Spitzen-Unternehmen der deutschen Wirtschaft durch Nicht-EU-Investoren übernommen werden sollen.[12]

16 Monate

können deutsche Unternehmen nach eigenen Angaben überleben, sollten sie Technologien oder Services nicht mehr aus den USA beziehen können.

↗Dataverse (2026)

Entscheidend ist, bei Schlüsseltechnologien unabhängig zu bleiben oder unabhängiger zu werden. Wir brauchen zwar weiterhin offene Märkte und Investitionen auch außerhalb der EU. Angesichts geopolitischer Spannungen muss aber gewährleistet sein, handlungsfähig zu bleiben. Insgesamt zeigt sich, dass das Interesse an europäischen Angeboten da ist. Europa muss digitale Technologien nicht nur entwickeln, sondern auch schneller skalieren und in die breite Anwendung bringen. Dafür braucht es eine innovationsfreundliche Regulierung, mehr Wachstumskapital und eine öffentliche Beschaffung, die europäischen Produkten eine Chance gibt. Digitale Souveränität ist jedoch nicht allein eine Aufgabe des Staates. Auch

[9] CASSIS Bonn, ↗»Digital Dependence Index (DDI)«.
[10] Bitkom e. V., ↗»Digitale Souveränität - wie beenden wir die Abhängigkeiten?«,2026.
[11] Bitkom e. V., ↗Presseinformation: Große Mehrheit wünscht sich digitale Technik, Software und Services aus Europa, 2026.
[12] Bitkom e. V., ↗Presseinformation; Digitale Souveränität: Mehr Schutz wichtiger Unternehmen gefordert, 2026.

Unternehmen und Zivilgesellschaft sind gefordert, auf vertrauenswürdige Lösungen zu setzen und digitale Kompetenzen gezielt auszubauen. Nur im Zusammenspiel aller Akteure lässt sich eine nachhaltige und selbstbestimmte digitale Zukunft sichern.

Kriterienkataloge zur Messung digitaler Souveränität

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) hat mit seinem Diskussionspapier von März 2026 Kriterien zur Bewertung der digitalen Souveränität der öffentlichen Verwaltung vorgelegt.[13] Insgesamt hat das ZenDiS dabei 20 Kriterien in den vier Kategorien Organisation und Fähigkeiten, Digitale Anwendungen und Dienste, Informationen und Daten sowie Betrieb und Infrastruktur vorgeschlagen.

Mit dem Cloud Sovereignty Framework der EU liegt ein erster Orientierungsrahmen zur Bewertung von Cloud-Angeboten vor. Im Framework werden acht zentrale Souveränitätsziele definiert, die benennen, in welchen Bereichen Cloud-Dienste europäischer Kontrolle unterliegen müssen, um als »souverän« zu gelten:
1. Strategische Souveränität, 2. Juristische Souveränität, 3. Daten- und KI-Souveränität, 4. Betriebliche Souveränität, 5. Lieferkettensouveränität, 6. technologische Souveränität, 7. Sicherheits- und Compliance-Souveränität und 8. ökologische Nachhaltigkeit. Ein zentrales Instrument in diesem Kontext ist die Klassifikation von Cloud-Diensten anhand sogenannter SEAL-Level (Sovereignty Effective Assurance Levels). Diese reichen von SEAL-0 bis SEAL-4 und beschreiben abgestuft, in welchem Maß ein Cloud-Dienst rechtlich, technisch und operativ unter europäischer Kontrolle steht.

Darauf aufbauend hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit den »Criteria enabling Cloud Computing Autonomy (C3A)« einen Kriterienkatalog veröffentlicht, der Teile des EU Cloud Sovereignty Frameworks in konkrete und überprüfbare Anforderungen übersetzt. Die Kriterien bewerten Cloud-Souveränität entlang von sechs Dimensionen: strategische, juristische, datenbezogene, betriebliche, lieferkettenbezogene und technologische Souveränität. Damit zeigt sich, dass das europäische Framework bereits heute auf nationaler Ebene konkretisiert und operationalisiert wird. Gleichzeitig ist davon auszugehen, dass entsprechende Kriterien künftig auch in weiteren regulatorischen, sicherheitsrelevanten und sektoralen Kontexten Anwendung finden werden.

Mit der Veröffentlichung des Tech Sovereignty Package im Juni 2026 hat die Europäische Kommission diesen Ansatz auf EU-Ebene weitergeführt. Besondere Bedeutung kommt dabei dem Cloud and AI Development Act (CADA) zu. Der Verordnungsvorschlag soll einen unionsweiten Rahmen zur Stärkung des europäischen Cloud- und KI-Ökosystems schaffen, unter anderem durch Cloud- und KI-Leadership-Initiativen, den beschleunigten Ausbau von Rechenzentrumskapazitäten, die Verringerung kritischer technologischer Abhängigkeiten und die Förderung souveräner Cloud- und KI-Angebote für den öffentlichen Sektor. Zugleich sieht CADA ein harmonisiertes »Union cloud computing sovereignty framework« mit vier Union

[13] ZenDiS, ↗»Kriterien zur Bewertung von Digitaler Souveränität, Diskussionspapier, sowie ZenDiS, Konsultationsprozess zu Souveränitätskriterien«, 2026.

Assurance Levels vor, anhand derer Cloud-Dienste auf unterschiedlichen Souveränitätsniveaus bewertet und anerkannt werden können. Für öffentliche Beschaffungen sollen diese Assurance Levels eine verbindliche Rolle spielen: Cloud-Dienste müssen grundsätzlich mindestens Union Assurance Level 1 erfüllen; bei Tätigkeiten mit Public-Order-Relevanz können je nach Risikobewertung höhere Levels erforderlich sein.

Die im Juli 2026 von Deutschland und Frankreich vorgelegte gemeinsame Definition digitaler Souveränität beschreibt digitale Souveränität als mehrdimensionales Konzept, das entlang von sechs Dimensionen strukturiert und durch zugehörige Kriterien operationalisiert wird (vgl. Kapitel 1). Im Zentrum stehen u. a. rechtliche Durchsetzungsmöglichkeiten, der Schutz sensibler Daten oder die Resilienz von Infrastrukturen. Zentrale Kriterien sind beispielsweise die Nutzung digitaler Produkte von Anbietern in der EU oder vertrauenswürdigen internationalen Partnerstaaten, der konsequente Einsatz von Open-Source-Lösungen und modularen Architekturen zur Vermeidung von Lock-in-Effekten sowie der gezielte Auf- und Ausbau eigener Recheninfrastrukturen für KI und Cloud-Computing.

Ein einheitlicher, verbindlich geltender Standard zur Messung digitaler Souveränität existiert derzeit weder auf Ebene der EU noch in Deutschland; mit CADA liegt jedoch erstmals ein legislativer Vorschlag für einen harmonisierten EU-Rahmen zur Bewertung souveräner Cloud-Dienste vor, der bestehende Ansätze wie SEAL, C3A und die ZenDiS-Kriterien perspektivisch regulatorisch ergänzen und überlagern kann.

3 Ziele: Welche Ziele sollten Deutschland und Europa verfolgen?

Digitale Souveränität zielt generell darauf ab, Unabhängigkeit von einzelnen Wirtschaftsräumen, Staaten und Unternehmen bei Bezug und Nutzung digitaler Technologien, Dienste und Plattformen herzustellen. Im Einzelnen geht es um:

- Eigene Fähigkeiten zur Entwicklung, Herstellung und Veredelung digitaler Schlüsseltechnologien, Dienste und Plattformen.
- Eigene Fähigkeiten zur Prüfung und Bewertung digitaler Technologien, Dienste und Plattformen unter Leistungs- und Sicherheitsaspekten.
- Fähigkeiten von Unternehmen, Verbrauchern und Verwaltungen, digitale Technologien und Lösungen sicher, selbstständig und selbstbestimmt einzusetzen.

- Hoheitliche Handlungsfähigkeit des Staats zum Schutz von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Kommunikation nach innen und außen.

Ein zentrales Ziel deutscher Souveränitätspolitik muss sein, in ausgewählten Schlüsseltechnologien weltweit einzigartige Fähigkeiten zu entwickeln und dauerhaft zu erhalten. Digitale Souveränität bedeutet nicht, in allen Technologien führend zu sein, sondern in für Deutschland strategisch besonders relevanten Bereichen, wie etwa Quantencomputing, Physical AI, Digital Health und autonomen Systemen, internationale Spitzenpositionen zu erreichen. Solche technologischen Spitzenfähigkeiten stärken nicht nur Innovations- und Wettbewerbsfähigkeit, sondern schaffen zugleich strategische Interdependenzen, die Deutschlands außen- und wirtschaftspolitische Handlungsfähigkeit erhöhen. Eine erfolgreiche Souveränitätspolitik baut damit gezielt eigene Stärken aus und schafft gleichzeitig die Voraussetzungen, auch in geopolitisch angespannten Zeiten selbstbestimmt handeln zu können.

Digitale Souveränität umfasst darüber hinaus die Fähigkeit, auf externen wirtschaftlichen oder technologischen Druck wirksam und abgestuft reagieren zu können. Deutschland und Europa müssen in der Lage sein, kritischen Abhängigkeiten vorzubeugen und im Bedarfsfall mit adäquatem Gegendruck reagieren zu können, um die eigenen Interessen wirksam zu schützen und durchzusetzen.

Bitkom setzt sich dafür ein, dass Deutschland und Europa diese Ziele mit Nachdruck verfolgen. Dabei kommen auf die unterschiedlichen Akteure, also Digitalwirtschaft, gewerbliche Anwender, Verbraucher und Staat, unterschiedliche Aufgaben zu.

Für die digitale Souveränität Europas ist es entscheidend, dass Deutschland und die EU einen europäischen Souveränitätsverbund aufbauen, der über die EU hinaus auch eng verbundene westeuropäische Partnerstaaten, wie das Vereinigte Königreich und Norwegen, umfasst.

4 Maßnahmen: Aktionsplan Digitale Souveränität

Die Voraussetzung für ein digital souveränes Deutschland und Europa sind wettbewerbsfähige und innovationsfreundliche Rahmenbedingungen. Dazu gehören weniger Bürokratie, eine innovationsfreundliche Regulierung und die stärkere Aktivierung von Venture Capital durch institutionelle Investoren. Der folgende Aktionsplan bündelt 15 zentrale Maßnahmen in unterschiedlichen Politikfeldern, mit denen Deutschland und Europa die digitale Souveränität gezielt stärken können:

1. Europäischen Binnenmarkt ausbauen

Der Binnenmarkt ist Europas größter wirtschaftlicher Vorteil, bleibt aber durch Fragmentierung und uneinheitliche Regeln hinter seinem Potenzial zurück. Um global wettbewerbsfähig zu bleiben, braucht es einen echten digitalen Binnenmarkt mit klaren, EU-weit einheitlichen Rahmenbedingungen: Dazu gehören weniger Bürokratie, der Abbau von Gold-Plating und mehr Rechtssicherheit durch einen kohärenten digitalen Rechtsrahmen. Politik und Regulierung müssen auf digitale Souveränität und Wettbewerbsfähigkeit ausgerichtet sein, damit Unternehmen grenzüberschreitend wachsen können. Nur durch weniger Bürokratie, klare Regeln und einheitliche Standards kann Europa sein wirtschaftliches Potenzial voll ausschöpfen, seine Innovationskraft stärken und in einer zunehmend geopolitisch angespannten Welt seine Interessen wirksam vertreten.

2. Digitale Souveränität von Bund, Ländern und Kommunen stärken

Bund, Länder und Kommunen müssen digitale Technologien selbstbestimmt auswählen, sicher einsetzen und weiterentwickeln können. Grundlage sind technologieoffene, wettbewerbsorientierte Ansätze mit klaren, diskriminierungsfreien Kriterien – etwa zu Interoperabilität, offenen Schnittstellen, Portabilität und Sicherheit. Ziel ist Wahlfreiheit statt Festlegung auf einzelne Produkte. Möchte man in besonders kritischen oder strategisch wichtigen Bereichen »Buy European« bzw. »Made-with-Europe«-Ansätze verfolgen, braucht es eine praxistaugliche Balance: Es geht darum, europäische Wertschöpfung zu stärken, ohne Wettbewerb und Innovation durch übermäßige Bürokratie bei der Nachweiserbringung zu bremsen. Entscheidend sind daher einfache und klare, verhältnismäßige und EU-weit einheitliche Kriterien. Digitale Souveränität der Verwaltung erfordert zudem resiliente IT-Infrastrukturen, klare Governance und bundesweit einheitliche, praxistaugliche Vergaberegeln. Nur so lassen sich Handlungsfähigkeit, Innovation und Wettbewerb langfristig sichern.

3. Cyberresilienz stärken und Angriffe wirksam abwehren

Die meisten Cyberangriffe auf deutsche Unternehmen lassen sich China und Russland zuordnen. Gleichzeitig nutzen kriminelle Akteure neue Möglichkeiten durch KI und andere Technologien, um Angriffe effizienter und schädlicher zu machen. IT- und Cybersicherheit muss daher zum Rückgrat der deutschen Sicherheitsarchitektur werden und physische, digitale sowie hybride Bedrohungen gemeinsam in den Blick nehmen. Erforderlich sind ein einheitlich hohes Sicherheitsniveau in Staat und Wirtschaft, ein intelligentes Cyberlagebild sowie die systematische Einbeziehung technologischer Trends in Bedrohungsanalysen. Dabei müssen europäische Cybersicherheitslösungen gezielt gestärkt werden, um einseitige Abhängigkeiten zu reduzieren und eigene technologische Handlungsfähigkeit aufzubauen. Auch Fähigkeiten zur aktiven Cyberabwehr können Teil eines souveränen Umgangs mit der wachsenden Bedrohungslage sein, sofern Zuständigkeiten klar geregelt, Eingriffe verhältnismäßig ausgestaltet und die Digitalwirtschaft frühzeitig und kooperativ eingebunden wird. Ziel ist es, Deutschlands Reaktionsfähigkeit zu stärken, im Ernstfall handlungsfähig zu bleiben und Schäden durch Cyberangriffe wirksam zu begrenzen.

4. Strategische und operative Unabhängigkeit als Grundlage der Verteidigungsfähigkeit ausbauen

Digitalisierungs- und Rüstungsprojekte dürfen das mögliche Risiko von strategischen und operativen Abhängigkeiten in einem möglichen Verteidigungsfall nicht verstärken. Um Abhängigkeiten von außereuropäischen Anbietern in der Zukunft zu vermeiden, sollten gezielte Investitionen in die sicherheitspolitischen Dimensionen von Schlüsseltechnologien wie Künstlicher Intelligenz, Robotik, Quantenrechnern und autonomen Systemen stark ansteigen. Die Bundesregierung hat in den vergangenen Jahren hierfür Organisationen auf Bundesebene gegründet, die organisatorisch und finanziell hierfür ausgebaut werden sollten. Innovative Akteure in der Rüstungswirtschaft sowie die Potenziale von Dual-Use sollten noch stärker gefördert werden, beispielsweise um die Bundeswehr durch die Expertise aus dem zivilen Gesundheitsbereich oder aus der Automobilindustrie zu befähigen. Schließlich müssen neue Planungen einer klaren Wirkungspriorität bis 2029 unterliegen, während kurzfristige Überlegungen zur Verteidigungsfähigkeit nicht außer Acht gelassen werden dürfen.

5. Rechenzentrumsstandort Deutschland stärken

Leistungsfähige Rechenzentren sind die Grundlage digitaler Souveränität, wirtschaftlicher Wettbewerbsfähigkeit und moderner KI-Ökosysteme. Sie bilden das Rückgrat der Digitalisierung und sichern, dass Datenverarbeitung und Wertschöpfung in Deutschland und Europa stattfinden. Deutschland sollte daher zu einem international wettbewerbsfähigen und investitionsfreundlichen Rechenzentrumsstandort werden. Dafür braucht es eine praxisnahe, innovationsfreundliche und europäisch harmonisierte Regulierung. Planungs- und Genehmigungsverfahren sollten vereinheitlicht, digitalisiert und beschleunigt werden, um den Ausbau zu erleichtern. Gleichzeitig ist eine Energiepolitik erforderlich, die Versorgungssicherheit, wettbewerbsfähige Strompreise und verlässliche Netzanschlüsse gewährleistet. Nur im Zusammenspiel dieser Faktoren lässt sich ein starker und nachhaltiger Digitalstandort sichern.

6. Fähigkeiten in der Mikroelektronik auf Spitzenniveau ausbauen

Mikroelektronik ist eine zentrale Voraussetzung digitaler Souveränität. Ohne leistungsfähige und vertrauenswürdige Halbleiter bleiben kritische Infrastrukturen, Anwendungen und Innovationen stark von außereuropäischen Akteuren abhängig. Deutschland und Europa sollten daher entlang der gesamten Wertschöpfungskette eigene Stärken ausbauen – von Forschung und Design über Fertigung bis hin zu Packaging und Materialien. Ziel ist es, mit Initiativen wie dem European Chips Act und IPCEIs Kompetenzen in strategischen Technologiefeldern zu stärken, Lieferketten resilienter zu machen und die Skalierung innovativer Unternehmen zu erleichtern. Eine wettbewerbsfähige europäische Mikroelektronik stärkt damit nicht nur Innovationskraft und Wettbewerbsfähigkeit, sondern auch Krisenfestigkeit, Versorgungssicherheit und digitale Handlungsfähigkeit.

7. Europas Cloud-Standort zukunftssicher gestalten

Cloud-Technologien sind die Grundlage für digitale Innovation, wirtschaftliche Resilienz und technologische Handlungsfähigkeit in Europa. Sie ermöglichen den Einsatz von KI, moderne Dateninfrastrukturen und skalierbare digitale Anwendungen. Ziel muss sein, leistungsfähige und vertrauenswürdige Cloud-Kapazitäten in Europa

auszubauen und gleichzeitig den Zugang zu weltweit führenden Technologien sicherzustellen. Dafür braucht es ein offenes und wettbewerbliches Cloud-Ökosystem, das auf Sicherheit, Interoperabilität, offenen Standards und Wahlfreiheit basiert. Europäische Initiativen zu Cloud-Souveränität sollten daher risikobasiert, innovationsfreundlich und verhältnismäßig ausgestaltet werden sowie technische und organisatorische Schutzmaßnahmen gleichermaßen berücksichtigen. Mit den kommenden europäischen Cloud- und Dateninitiativen gilt es nun, regulatorische Fragmentierung zu vermeiden und die Rahmenbedingungen konsequent auf Innovation, Sicherheit und internationale Wettbewerbsfähigkeit auszurichten.

8. KI zum strategischen Souveränitätsfaktor machen

Die Entwicklung und breite Anwendung von Künstlicher Intelligenz ist zentral für Resilienz und digitale Souveränität in Europa. KI ist eine Schlüsseltechnologie mit enormem globalem Wertschöpfungspotenzial, das maßgeblich über künftige Wettbewerbsfähigkeit entscheidet. Ein relevanter Anteil dieser Wertschöpfung sollte in Europa entstehen. Ziel soll sein, den Ausbau leistungsfähiger KI-Fähigkeiten auf Spitzenniveau entlang der gesamten Wertschöpfungskette zu fördern; von Rechenkapazitäten und Dateninfrastrukturen bis hin zu skalierbaren Anwendungen. Dafür braucht es ein offenes, innovationsfreundliches Ökosystem, das internationale Zusammenarbeit stärkt und europäische Stärken gezielt weiterentwickelt. Bei der Umsetzung des AI-Acts nach Änderung durch den AI-Omnibus, gilt es nun, die regulatorischen Hürden so niedrig wie möglich zu halten und die Rahmenbedingungen klar auf Innovation und Skalierung auszurichten. Gerade mit Blick auf die Entwicklung leistungsfähiger allgemeiner KI-Systeme (AGI) wird deutlich, dass sich Wertschöpfung, Marktanteile und technologische Führungspositionen künftig noch stärker auf wenige globale Akteure konzentrieren könnten. Um langfristig wettbewerbsfähig zu bleiben und strategische Abhängigkeiten zu reduzieren, muss Europa deshalb gezielt in eigene KI-Fähigkeiten und skalierbare Innovationsökosysteme investieren.

9. Industrial AI für digitale Souveränität skalieren

KI ist zunehmend ein integraler Bestandteil von Industrie-4.0-Anwendungen, insbesondere in datenintensiven Feldern wie der vorausschauenden Wartung und der Qualitätssicherung. Deutschland und Europa sollten Industrial AI daher gezielt entwickeln, skalieren und in die Breite der industriellen Anwendung bringen. Entscheidend ist, KI systematisch in Produktions- und Engineering-Prozesse zu überführen. Für den Hochlauf industrieller KI muss Deutschland die Standortbedingungen verbessern, etwa durch ausreichende Rechenkapazitäten, funktionierende Datenökosysteme entlang der Wertschöpfungskette, praxistaugliche Regulierung sowie gezielte Fachkräfte- und Förderangebote für den Mittelstand. Nur so kann Industrial AI Wettbewerbsfähigkeit und damit auch technologische Souveränität stärken.

10. Forschungs- und Innovationspolitik auf digitale Souveränität ausrichten

Deutschland hat bei vielen Schlüsseltechnologien des 20. Jahrhunderts Maßstäbe gesetzt, droht jedoch bei den digitalen Schlüsseltechnologien des 21. Jahrhunderts den Anschluss zu verlieren. Die Forschungs- und Innovationspolitik muss daher konsequent auf den Hochlauf digitaler Schlüsseltechnologien ausgerichtet und die Hightech-Agenda schnell, klar priorisiert und verbindlich umgesetzt werden. Entscheidend sind ein stärkerer Wissenstransfer in die Anwendung, ein wettbewerbsfähiges digitales

Ökosystem für Aufbau und Skalierung, die Berücksichtigung von Dual-Use-Potenzialen sowie der Staat als Ankerkunde. Zudem braucht es eine enge Verzahnung mit der europäischen Forschungs- und Wirtschaftspolitik – etwa durch einen zielgerichteten European Competitiveness Fund, ein starkes Horizon-Europe-Nachfolgeprogramm, bessere Bedingungen für Kapitalmobilisierung und eine spürbare Entbürokratisierung der Forschungsförderung durch digitalisierte, schlanke Verfahren. Eine Absicherung unserer Forschungseinrichtungen und -ergebnisse ist dabei zentral, um technologische Abhängigkeiten zu reduzieren, sensible Kompetenzen zu schützen und die Digitale Souveränität Deutschlands nachhaltig zu stärken.

11. Europa als Wachstumsmarkt für innovative Startups entwickeln

In einer immer härter umkämpften Welt muss Europa der beste Standort für Startups und Scaleups werden. Nur mit konkurrenzfähigen Tech-Unternehmen bleibt die EU politisch handlungsfähig. Deutschland, als größte Volkswirtschaft, sollte mit besonderem Ehrgeiz vorangehen und Gründung, Wachstum sowie Internationalisierung zur Normalität machen. Dafür braucht es weniger Bürokratie in der Frühphase, verbesserten Zugang zu (institutionellem) Kapital und klare Exit-Pfade. Zudem sollten die Mitgliedstaaten eine schnelle, einheitliche Umsetzung europäischer Initiativen vorantreiben, etwa die EU Inc. oder die Vollendung der Kapitalmarktunion durch die Savings- und Investment-Union.

12. Außenwirtschaftspolitik entlang digitaler Souveränität neu aufstellen

Die internationale Vernetzung der deutschen Wirtschaft bleibt ein zentraler Erfolgsfaktor. Auch die Nationale Wirtschaftsschutzstrategie vom März 2026 ist ein wichtiger erster Schritt. Europäische Wirtschaftsschutzinstrumente sollten gezielt und verhältnismäßig eingesetzt werden, um faire Wettbewerbsbedingungen zu sichern, Verzerrungen abzuwehren und europäische Wertschöpfung zu schützen. Die Europäische Union muss in der Lage sein, auf externen wirtschaftlichen Druck gegenüber ihren Mitgliedstaaten – insbesondere in technologisch sensiblen Bereichen – adäquat, abgestuft und wirksam zu reagieren. Erforderlich ist zudem eine China-Politik auf Augenhöhe, die Kooperation ermöglicht und zugleich Marktmissbrauch sowie kritische Abhängigkeiten adressiert. Auch im transatlantischen Verhältnis gilt es, digitale Kooperationschancen zu nutzen und gleichzeitig den europäischen Ordnungsrahmen zu wahren. Deutschland sollte darüber hinaus gemeinsam mit der EU das Bewusstsein für eigene strategische Hebel im digitalen Raum stärken und die politische Handlungsfähigkeit im Bedarfsfall sichern.

13. Resilienz und Souveränität durch Open Source stärken

Open Source stärkt die digitale Souveränität Deutschlands und Europas durch offene, kollaborative Entwicklung, die Innovation beschleunigt und Ressourcen effizient nutzt. Transparenter Quellcode erhöht Sicherheit und Vertrauen, während offene Standards und Interoperabilität Flexibilität fördern und Abhängigkeiten von einzelnen Anbietern reduzieren. Voraussetzung ist eine nachhaltige Finanzierung von Wartung, Sicherheit und Resilienz kritischer Infrastrukturen. Ergänzend können gezielte Anreize für die Privatwirtschaft – etwa steuerliche Förderung analog zu F&E-Instrumenten – die Verbreitung von Open Source unterstützen.

14. Digitale Selbstbestimmung sichern, Datenschutz innovationsfreundlich gestalten

Der Schutz personenbezogener Daten ist ein zentraler Bestandteil digitaler Souveränität und umfasst auch die Selbstbestimmung der Bürgerinnen und Bürger über ihre Daten und digitale Identität. Datenschutz muss dabei innovationsfreundlich, praxisnah und kohärent umgesetzt werden, um Vertrauen und Wettbewerbsfähigkeit gleichermaßen zu stärken. Die DSGVO schafft seit 2018 ein Level-Playing-Field für Anbieter in der EU und fördert durch Art. 25 Anonymisierungs- und Pseudonymisierungstechnologien sowie Transparenzprinzipien. In der Praxis bestehen jedoch weiterhin Unsicherheiten, etwa durch uneinheitliche Auslegung, restriktive Anwendung von Datensparsamkeit und Zweckbindung sowie hohe Dokumentationsanforderungen. Es ist daher eine kohärente Datenpolitik erforderlich.

15. Die Gesellschaft souverän, resilient und zukunftsfähig aufstellen

Der digitale Raum ist ein gesellschaftlicher Raum. Digitale Souveränität muss daher immer auch als gesellschaftliche Souveränität verstanden werden. Zentrale Voraussetzung sind digitale Kompetenzen, bei denen Deutschland international zurückliegt: Nur 26 Prozent der Deutschen trauen sich zu, Falschinformationen zu erkennen. Im Bitkom-DESI liegt Deutschland im EU-Vergleich beim Indikator zu Kompetenzen nur auf Platz 15 von 27. Notwendig ist eine breit angelegte Offensive zur Stärkung digitaler Kompetenzen in allen Altersgruppen, etwa durch eine Bundeszentrale für Digitale Bildung. Zudem braucht es verpflichtenden Informatikunterricht ab Klasse 5 in allen Bundesländern. Digitale Souveränität erfordert auch verlässliche Infrastruktur in allen Bildungseinrichtungen. Statt kurzfristiger Förderprogramme braucht es langfristige Strategien und eine dauerhafte Finanzierung über die Kernhaushalte von Bund und Ländern.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartnerin
Janine Jahreiß | Leiterin Digitale Souveränität, Infrastruktur & Regulierung
T +49 151 27631531 | j.jahreiss@bitkom.org

Verantwortliches Bitkom-Gremium
Bitkom Präsidium

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.