

Positionspapier der Business Software Alliance (BSA) zur digitalen Souveränität in Deutschland und Europa

1. Einleitung:

Digitale Souveränität im politischen und wirtschaftlichen Kontext

Digitale Souveränität hat in den vergangenen Jahren deutlich an Bedeutung gewonnen. Das zugrunde liegende Konzept ist zwar nicht neu. Doch geopolitische Verschiebungen, wachsende sicherheitspolitische Spannungen und die digitale Transformation kritischer Infrastrukturen rücken das Thema zunehmend in den Mittelpunkt politischer und wirtschaftlicher Strategien. Sowohl die Europäische Union als auch Deutschland verfolgen das Ziel, digitale Abhängigkeiten zu verringern, die Resilienz ihrer digitalen Infrastrukturen zu erhöhen und mehr Handlungsfähigkeit im digitalen Raum zu erlangen.

Trotz der hohen politischen Aufmerksamkeit existiert bislang keine allgemein anerkannte Definition von digitaler Souveränität. Verschiedene Institutionen und Akteure setzen unterschiedliche Schwerpunkte:

- Die **Europäische Parlamentarische Forschungsstelle (EPRS)** [beschreibt](#) digitale Souveränität als die Fähigkeit Europas, im digitalen Raum eigenständig zu agieren – unter anderem durch den Schutz eigener Interessen und die Förderung von Innovation.
- Der **Bundesbeauftragte der Bundesregierung für Informationstechnik** [versteht](#) darunter die Fähigkeit von Individuen und Institutionen, sicher und eigenverantwortlich im digitalen Raum zu handeln. Dies erfordere moderne, vertrauenswürdige IT, geringere Abhängigkeiten von Anbietern sowie offene und wettbewerbsfreundliche Märkte.
- Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** [betont](#), dass digitale Souveränität keine vollständige Autarkie bedeutet. Vielmehr sei eine Doppelstrategie notwendig: der Ausbau europäischer Technologien bei gleichzeitiger sicherer Einbindung internationaler Lösungen.
- Die **Digitalwirtschaftsvereinigung Bitkom** [definiert](#) digitale Souveränität als die Fähigkeit zur selbstbestimmten Handlung im digitalen Raum – mit Fokus auf Anbieterunabhängigkeit, Interoperabilität und die Vermeidung von Lock-in-Effekten, ohne jedoch vollständige Selbstversorgung anzustreben.
- Für das **Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS)** [bedeutet](#) Digitale Souveränität die Fähigkeit von Staat und Organisationen, digitale Infrastrukturen und Dienste eigenständig, selbstbestimmt und sicher zu betreiben und weiterzuentwickeln – ohne unkontrollierbare Abhängigkeiten von einzelnen Anbietern oder Drittstaaten. Dazu gehören neben der Datensouveränität auch rechtssicherer und DSGVO-konformer Betrieb, technologische Kontrolle und Gestaltungsfähigkeit, Wechselfähigkeit ohne Vendor-Lock-in, Transparenz etwa durch offenen Quellcode sowie die Möglichkeit zur Anpassung und Weiterentwicklung. Nur wenn all diese Aspekte zusammen erfüllt sind, sei ein Höchstmaß an Digitaler Souveränität gewährleistet.

Diese unterschiedlichen Perspektiven verdeutlichen: Digitale Souveränität ist ein facettenreiches Konzept, das technische, wirtschaftliche, rechtliche und gesellschaftliche Aspekte vereint. In der politischen und gesellschaftlichen Diskussion über digitale Souveränität treten unterschiedliche Motive hervor. Sie reichen vom Schutz personenbezogener Daten und der Stärkung der Cybersicherheit über die Sicherung von Resilienz und Ausfallsicherheit digitaler Infrastrukturen bis hin zu wirtschaftlichen Überlegungen wie der Vermeidung von Lock-in-Effekten, dem Schutz sensibler Geschäftsdaten oder dem Ausbau eigener Technologie-Infrastrukturen. Vor diesem Hintergrund möchte die BSA mit diesem Positionspapier zur sachlichen Diskussion beitragen und ihre Sichtweise als internationale Branchenvertretung einbringen, insbesondere in Gesprächen mit Entscheidungsträgern.

2. Nationale Perspektive: Digitale Souveränität in der deutschen Digitalpolitik

In Deutschland gilt digitale Souveränität als zentrales Element der Digitalpolitik der Bundesregierung. Im [Koalitionsvertrag](#) von CDU/CSU und SPD wird sie explizit als politisches Ziel benannt: „*Unsere Digitalpolitik ist ausgerichtet auf Souveränität, Innovation und gesellschaftlichen Fortschritt. Digitalpolitik ist Machtpolitik. Wir wollen ein digital souveränes Deutschland.*“

Die Bundesregierung verfolgt dazu mehrere strategische Ansätze:

- **Verringerung technologischer Abhängigkeiten** durch den Ausbau europäischer Schlüsseltechnologien wie Cloud, Künstliche Intelligenz, Halbleitertechnologien und Cybersicherheit.
- **Stärkung offener, interoperabler Infrastrukturen**, beispielsweise durch Initiativen wie den „Deutschland Stack“ oder die „Deutsche Verwaltungscloud“.
- **Förderung von Forschung und Technologietransfer**, insbesondere durch Unterstützung von Start-ups, angewandter KI, Reallaboren und digitaler Bildung.
- **Integration von Souveränitätskriterien** in die öffentliche Beschaffung durch neue Vergabekriterien und standardisierte Bewertungsmodelle.
- **Verbesserung der Dateninfrastruktur** durch klare gesetzliche Rahmenbedingungen für Datenzugang, Datentreuhand und offene Verwaltungsdaten („Public Money, Public Data“).
- **International abgestimmte Regulierungsansätze** mit dem Ziel, europäische Standards in den Bereichen Vertrauen, Datenschutz und Wettbewerbsfähigkeit global zu verankern.

Aus Sicht der BSA ist positiv hervorzuheben, dass Deutschland digitale Souveränität nicht isoliert betrachtet, sondern in Verbindung mit Innovation, Marktzugang und internationaler Wettbewerbsfähigkeit. Die Herausforderung besteht darin, Sicherheitsinteressen und offene Marktstrukturen in ein ausgewogenes Verhältnis zu bringen.

Dabei gewinnt ein differenzierter, risikobasierter Ansatz an Bedeutung. Dabei sollten ganze Technologien oder Branchen nicht pauschal betrachtet werden, sondern sich, ähnlich wie im EU AI Act, an der Sensibilität konkreter Anwendungsbereiche und der Art der verarbeiteten Daten orientieren. Zusätzliche Sicherheitslayer sind vor allem dort relevant, wo besonders schützenswerte Informationen verarbeitet

werden, nicht jedoch flächendeckend für alle Cloud- oder KI-Anwendungen. Eine unspezifische Ausweitung von Souveränitätsanforderungen kann dabei die Innovationskraft hemmen und Investitionsentscheidungen in Deutschland erschweren.

Viele internationale Anbieter unterstützen diese Ziele bereits, etwa durch Investitionen in lokale Rechenzentren, Partnerschaften mit deutschen Unternehmen, technische und organisatorische Maßnahmen zur Datenlokalisierung oder rechtliche Zusicherungen zur Dienstkontinuität und datenrechtskonformen Verarbeitung.

3. Positionierung der BSA: Für ein souveränes, offenes und innovationsfähiges Europa

Die Business Software Alliance (BSA) repräsentiert weltweit führende Unternehmen der Softwarebranche. Unsere Mitglieder stammen aus unterschiedlichen Weltregionen. Diese globale Perspektive spiegelt sich auch in unserem Verständnis von digitaler Souveränität wider: Wir erkennen das berechtigte Interesse Deutschlands und Europas an, technologische Unabhängigkeit zu stärken, digitale Infrastrukturen zu schützen und kritische Systeme vertrauenswürdig zu gestalten.

Ein inklusives Verständnis von digitaler Souveränität

Aus Sicht der BSA sollte digitale Souveränität nicht durch geografische Abgrenzung definiert werden, sondern vor allem durch die Fähigkeit von Staaten, Unternehmen und Individuen, eigenverantwortlich über ihre digitale Infrastruktur, Daten und Technologien zu entscheiden. Dies lässt sich sowohl durch den Aufbau europäischer Kapazitäten als auch durch vertrauensvolle Zusammenarbeit mit internationalen Partnern erreichen, vorausgesetzt, gemeinsame Anforderungen an Sicherheit, Datenschutz, Transparenz sowie Interoperabilität werden erfüllt.

Ein solcher Ansatz verbindet strategische Resilienz mit globaler Innovationskraft. Die Möglichkeit, aus unterschiedlichen Anbietern wählen zu können, sollte im Vordergrund stehen, denn Vielfalt im Markt stärkt die Widerstandsfähigkeit digitaler Systeme. Eigenständigkeit entsteht nicht durch „Buy European“-Vorgaben, sondern durch wettbewerbsfreundliche Rahmenbedingungen, die Interoperabilität, Transparenz und Sicherheit aller angebotenen Lösungen fördern – unabhängig von der Herkunft der Technologie. Digitale Handlungsfähigkeit bedeutet nicht Abschottung, sondern klare Regeln, angemessene Standards und verlässliche internationale Kooperation.

Beitrag globaler Unternehmen zur digitalen Souveränität Europas

BSA-Mitglieder tragen bereits aktiv zur Umsetzung europäischer Zielsetzungen bei – etwa durch Investitionen in lokale Infrastruktur, Kooperationen bei der Entwicklung souveräner Cloud-Lösungen oder durch technisch, rechtlich und organisatorisch abgesicherte Dienste. Beispiele sind europäische Datenräume, verschlüsselungskontrollierte Technologien oder die lokale Beschäftigung von Fachkräften. Solche Partnerschaften stärken Vertrauen, lokales Know-how und rechtliche Sicherheit.

BSA-Mitglieder sind zudem führend im Bereich der IT-Sicherheit und ermöglichen es europäischen Kunden, durch die Nutzung dieser sicheren Anwendungen ihre digitale Souveränität weiter zu stärken. Diese Aktivitäten und Kooperationen zeigen, dass internationale Unternehmen die digitale Souveränität Europas konstruktiv mitgestalten können – als Teil eines gemeinsamen, offenen digitalen Ökosystems.

Europa als aktiver Gestalter seiner digitalen Zukunft

Die BSA würdigt das Ziel Europas, seine digitale Zukunft eigenständig zu gestalten. Der Aufbau eigener Technologien, der Ausbau digitaler Infrastrukturen, die Wahrung hoher Datenschutzstandards und die Integration von Souveränitätsaspekten in die Beschaffung sind nachvollziehbare politische Maßnahmen.

Gleichzeitig spricht sich die BSA für eine offene, nichtdiskriminierende Marktordnung aus. Einheitliche und transparente Anforderungen an Sicherheit, Vertrauen und Rechtsstaatlichkeit können dazu beitragen, dass sowohl europäische als auch internationale Anbieter auf fairer Grundlage zur Umsetzung dieser Ziele beitragen.

Narrativ der technologischen Abhängigkeiten

In der aktuellen Debatte zur digitalen Souveränität werden gelegentlich technologische Abhängigkeiten mit potenziellen Zugriffsbeschränkungen ins Feld geführt, also die Vorstellung, dass außereuropäische Cloud-Anbieter, insbesondere mit Sitz in den USA, europäische Kunden in Krisensituationen gezielt von ihren Diensten abschneiden könnten. Aus Sicht der BSA greift dieses Narrativ zu kurz und lenkt von den eigentlichen Herausforderungen ab. Die Beziehungen zwischen Cloud-Anbietern und ihren Kunden beruhen auf vertraglichen Verpflichtungen, die rechtlich bindend sind. Eine willkürliche Zugriffsbeschränkung von Diensten hätte erhebliche wirtschaftliche und rechtliche Konsequenzen, sowohl für Anbieter als auch für betroffene Kunden. Zudem ist die technische Infrastruktur moderner Cloud-Dienste redundant, verteilt und dezentral aufgebaut. Rechenzentren in der EU, betrieben von rechtlich eigenständigen Tochtergesellschaften unter europäischem Recht, tragen zusätzlich zur Stabilität und Verlässlichkeit der Dienste bei.

Entscheidend für digitale Resilienz ist nicht die Herkunft des Anbieters, sondern die Fähigkeit von Unternehmen und öffentlichen Stellen, ihre digitale Infrastruktur strategisch abzusichern. Dazu gehören unter anderem Multi-Cloud-Ansätze, hybride Cloud-Modelle, Datenportabilität und Notfallstrategien. Auch europäische Anbieter sind nicht automatisch frei von Risiken wie Cyberangriffen, Systemausfällen oder wirtschaftlicher Instabilität. Ein hoher Grad an Cybersicherheit setzt robuste technische und organisatorische Schutzmaßnahmen voraus – etwa geprüfte Sicherheitsarchitekturen und einheitliche Standards. Eine einseitige Fokussierung auf Nationalität kann daher zu einer trügerischen Sicherheit führen, insbesondere im Hinblick auf Cybersicherheit und Resilienz: Denn die effektive Abwehr globaler Cyberbedrohungen – eine Grundbedingung für digitale Souveränität – erfordert einen weltweiten Zugang zu Bedrohungsdaten und verteilte Netzwerkinfrastrukturen mit ausreichend Kapazitäten. Digitale Souveränität entsteht nicht durch protektionistische Abschottung, sondern durch regulatorische Klarheit, die Ermöglichung eines sicheren, grenzüberschreitenden Datenverkehrs, technische Redundanz und unternehmerische Verantwortung. Die BSA spricht sich daher für eine resilienzorienteerte Digitalstrategie aus, die auf Diversität, Interoperabilität, Partnerschaft sowie auf klare Sicherheitsstandards setzt – damit den Dreiklang aus Standards, Kooperation und offenen Märkten stärkt und nicht auf Isolation fußt.

4. Ausblick und Einordnung

Die BSA befürwortet ein Europa, das digitale Souveränität nicht durch Ausgrenzung, sondern durch Standards, Kooperation und offene Märkte verwirklicht. Digitale Eigenständigkeit und internationale Zusammenarbeit schließen sich nicht aus, im Gegenteil: Unter den richtigen politischen Rahmenbedingungen können sie sich gegenseitig stärken. Digitale Souveränität sollte dabei als die

BSA: Positionspapier zur digitalen Souveränität in Deutschland und Europa

Fähigkeit verstanden werden, digitale Ressourcen risikobasiert auszuwählen und zu steuern – durch Förderung von Transparenz, Sicherheit und Innovationsfähigkeit. Flexible, technologieneutrale Zertifizierungen auf Grundlage objektiver technischer Kriterien sowie vertrauensvolle Partnerschaften können langfristig zur Stärkung der Cybersicherheit und der Wettbewerbsfähigkeit Europas beitragen und somit zur digitalen Souveränität.

Darüber hinaus kann die strategische Nutzung bestehender technischer Standards einen wichtigen Beitrag zur digitalen Souveränität leisten. Statt neue europäische oder deutsche Normen von Grund auf zu entwickeln, sollten bewährte internationale Standards übernommen und kontextualisiert werden. Dies würde nicht nur die Interoperabilität fördern, sondern auch die Einführung sicherer Technologien beschleunigen und Ressourcen für wirklich neue Entwicklungen freisetzen. Die BSA spricht sich daher für eine Standardisierungspolitik aus, die auf Kompatibilität, Effizienz und globale Anschlussfähigkeit setzt – und so Standards, Kooperation und offene Märkte fördert.

Die BSA steht bereit, diesen Weg partnerschaftlich zu begleiten.

