Datensicherheit und digitale Souveränität: Grundlagen nachhaltiger Wettbewerbsfähigkeit

Europas Unternehmen stehen vor einer doppelten Herausforderung: Sie wollen einerseits mit dem globalen Innovationstempo Schritt halten und andererseits die Kontrolle über ihre sensiblen Daten bewahren. Datensicherheit und digitale Souveränität sind dabei längst keine rein technischen Fragen mehr. Sie bilden die strategische Grundlage für Vertrauen, Rechtssicherheit und langfristige Wettbewerbsfähigkeit.

Wachsende Abhängigkeiten und Cyberrisiken

Aktuelle Entwicklungen machen deutlich, wie verletzlich digitale Wertschöpfung geworden ist. Cyberangriffe auf kritische Infrastrukturen, Sabotage in Lieferketten und gezielte Datenmanipulation entfalten reale wirtschaftliche Wirkung. Gleichzeitig dominieren außereuropäische Cloud-Anbieter weiterhin große Teile des Markts – eine Konzentration, die strukturelle Abhängigkeiten schafft, die weit über technische Aspekte hinausgehen.

Laut aktuellem Bitkom Cloud Report halten 78 Prozent der deutschen Unternehmen Deutschland für zu abhängig von US-Anbietern. Und das Analystenhaus Gartner geht davon aus, dass bis 2030 mehr als 75 Prozent der europäischen Unternehmen ihre virtuellen Workloads in Lösungen überführen werden, die geopolitische Risiken gezielt reduzieren. Zum Vergleich: Im Jahr 2025 haben das weniger als fünf Prozent getan.

Der US CLOUD Act macht das Thema greifbar: Er verpflichtet amerikanische Unternehmen, gespeicherte Daten auf Anfrage an US-Behörden herauszugeben, auch wenn sich diese physisch in Europa befinden. Damit gibt jede Organisation, die auf US-basierte Dienste setzt, einen Teil ihrer Kontrolle über vertrauliche Informationen ab. Immer mehr europäische Unternehmen stellen sich daher die kritische Frage: Wer hat tatsächlich Zugriff auf die eigenen Daten und wo sind sie gespeichert?

Digitale Souveränität wird so zur Frage der Selbstbestimmung: Organisationen, die eigene Handlungsspielräume sichern wollen, entscheiden sich bewusst für IT-Infrastrukturen und Rechtsrahmen, die europäischen Werten und Gesetzen entsprechen.

Transparenz, Zugriffsrechte und Nachvollziehbarkeit

Wer sensible Daten wie Konstruktionsunterlagen, Stücklisten oder Projektdokumentationen verwaltet, profitiert von klaren Strukturen für Zugriffsrechte und Verantwortlichkeiten. Ein präzises Rollen- und Berechtigungskonzept legt fest, wer welche Informationen einsehen, bearbeiten oder freigeben darf. Jede Änderung bleibt nachvollziehbar, jeder Workflow dokumentiert.

Versionshistorien und die Möglichkeit, ältere Dokumentenstände wiederherzustellen, schaffen Transparenz über den gesamten Informationslebenszyklus. Dies betrifft auch die Zusammenarbeit

mit externen Partnern, Lieferanten oder Kunden entlang komplexer Lieferketten. Compliance-Anforderungen lassen sich auf diese Weise effizient erfüllen, ohne betriebliche Abläufe zu belasten.

Entscheidend ist dabei die Balance: Zusammenarbeit über Unternehmensgrenzen hinweg gelingt nur dann nachhaltig, wenn sie auch den Schutz vertraulicher Informationen umfasst. Automatisierte Freigabeprozesse und ein granulares Rechtemanagement bilden dafür wesentliche Bausteine.

Künstliche Intelligenz: Chancen und Risiken für die Datensouveränität

Künstliche Intelligenz verändert das digitale Informationsmanagement grundlegend. Richtig eingesetzt, steigert sie Effizienz und Qualität erheblich, etwa durch automatisierte Klassifizierung von Dokumenten, intelligente Suchfunktionen oder Unterstützung bei mehrsprachiger Kommunikation. Generative Sprachmodelle zeigen eindrucksvoll, wie leistungsfähig KI-Systeme heute sind.

Gleichzeitig birgt der unkontrollierte Einsatz von KI Risiken für die Datensouveränität. Viele öffentlich zugängliche Sprachmodelle verarbeiten eingegebene Informationen auf Servern außerhalb des europäischen Rechtsraums. Nutzer:innen können oft nicht nachvollziehen, wie ihre Daten weiterverarbeitet oder für das Training zukünftiger Systeme genutzt werden. Für Organisationen, die mit vertraulichen oder geschäftskritischen Informationen arbeiten, entsteht daraus ein erhebliches Risiko.

Eine wirkungsvolle Alternative bieten mandantenreine KI-Modelle, die in abgeschotteten, europäischen Umgebungen ohne Internetanbindung laufen. Solche Systeme lernen ausschließlich aus den Daten der jeweiligen Organisation und geben keinerlei Informationen nach außen weiter. KI und Datenschutz schließen sich damit keineswegs aus – die entscheidende Voraussetzung ist eine Implementierung mit der nötigen Sorgfalt und innerhalb eines klar definierten rechtlichen Rahmens.

Europäische Cloud-Infrastruktur als Fundament

Digitale Selbstbestimmung baut auf Infrastruktur, die europäischen Werten, Gesetzen und Datenschutzprinzipien folgt. Vollständig in Europa betriebene Cloud-Plattformen schaffen diese Grundlage: Datenhaltung, Entwicklung und Betrieb unterliegen dem europäischen Rechtsrahmen und gestalten sich damit transparent, überprüfbar und sicher.

Unternehmen profitieren dabei nicht nur von rechtlicher Klarheit, sondern auch von der technischen Flexibilität moderner Cloud-Architekturen. Wer den Datenstandort gezielt wählen und kontrollieren kann, stärkt das Vertrauen in die eigene digitale Infrastruktur und reduziert strukturelle Abhängigkeiten von außereuropäischen Anbietern spürbar.

Zertifizierte Sicherheit als Vertrauensbasis

Digitale Souveränität erfordert auch überprüfbare Sicherheitsstandards. Anerkannte Zertifizierungen und Testate – etwa nach BSI C5, ISO 27001/27018, ISAE 3000 SOC2 oder dem EU Cloud Code of Conduct – machen Datenschutz und Informationssicherheit messbar und vergleichbar.

Regelmäßige, unabhängige Audits schaffen Transparenz und Nachvollziehbarkeit. Organisationen wissen damit genau, unter welchen Bedingungen ihre Daten verarbeitet werden – ein wesentlicher Faktor, um Vertrauen innerhalb globaler Wertschöpfungsketten zu festigen und Compliance-Anforderungen dauerhaft zu erfüllen.

Handlungsspielräume zurückgewinnen: Autonomie durch Low-Code und No-Code

Digitale Souveränität endet nicht bei der Infrastruktur. Sie zeigt sich auch in der Fähigkeit, Prozesse eigenständig zu gestalten. Low-Code- und No-Code-Ansätze ermöglichen es Fachabteilungen, Abläufe selbst zu modellieren und Workflows anzupassen, ohne tiefgreifende Programmierkenntnisse oder Abhängigkeit von externen Dienstleistern.

Unternehmen entscheiden so selbst, welche Datenflüsse sie zulassen, welche Sicherheitsrichtlinien sie implementieren und wie sie ihre Abläufe gestalten. Diese technische Selbstbestimmung ist ein direkter Ausdruck digitaler Souveränität und stärkt gleichzeitig Reaktionsfähigkeit und Innovationskraft.

Fazit: Souveränität als strategische Entscheidung

Datensicherheit und digitale Souveränität sind weit mehr als technische Schutzmaßnahmen. Sie stehen für Eigenständigkeit, Innovationskraft und die Bereitschaft, Verantwortung für das eigene Wissen zu übernehmen. Organisationen, die Datenhoheit, Compliance und betriebliche Effizienz miteinander verbinden, legen den Grundstein für eine zukunftsfähige digitale Strategie.

Europas Unternehmen gestalten ihre digitale Zukunft dann am wirkungsvollsten, wenn sie Technologien einsetzen, die Kontrolle und Fortschritt gleichermaßen ermöglichen. Eine souveräne Datenstrategie schafft Resilienz gegenüber äußeren Einflüssen und sichert langfristig den wirtschaftlichen Erfolg. Wer heute in digitale Eigenständigkeit investiert, investiert in die Wettbewerbsfähigkeit von morgen.

Autor

Andreas Dangl ist Entrepreneur und Geschäftsführer der Fabasoft Approve GmbH. In seiner Funktion unterstützt er Unternehmen aus der Industrie bei der Einführung von KI-gestütztem Dokumenten- und Qualitätsmanagement. www.fabasoft.com/approve