

Datensouveränität ist heute ein strategisches Thema auf Vorstandsebene. Geopolitische Instabilität und Risiken durch IT-Abhängigkeiten sind die treibenden Faktoren. Die praktische Antwort darauf ist eine Architektur, die mehrschichtig, portabel und auf Resilienz ausgerichtet ist.

Cloud ohne Kompromisse: Datensouveränität mit einem resilienzorientierten und risikomindernden Ansatz in Ihre Infrastruktur integrieren

Mai 2026

Geschrieben von: Archana Venkatraman, Senior Research Director, Cloud Data Management

Einleitung

Das operative Umfeld für Organisationen in EMEA im Jahr 2026 lässt sich am besten als fragil, angespannt, unsicher und nichtlinear beschreiben. Vor diesem Hintergrund lautet die übergeordnete Aufgabe digitale Souveränität: die Fähigkeit von Staaten, Organisationen und Einzelpersonen, ihre Daten, Infrastruktur und Fähigkeiten frei von externer Einflussnahme zu steuern, wie IDC sie definiert. Organisationen in EMEA sehen sich mit einem regulatorischen Umfeld konfrontiert, das sich schneller verändert als Beschaffungszyklen. Geopolitische Turbulenzen, sich überlagernde Regulierungen, steigende Anforderungen durch KI sowie die strukturelle Konzentration auf wenige Hyperscaler haben eine grundlegende Schwachstelle offengelegt. Organisationen können die rechtlichen und regulatorischen Rahmenbedingungen eines Landes nur selten kontrollieren. Sie können jedoch steuern, wo ihre Daten liegen und wie sie verwaltet werden.

Diese Abhängigkeiten haben systemische Folgen und bergen Risiken für die Business Continuity. Dadurch wird die Souveränität von einem Nice-to-have und Anliegen der Rechtsabteilung zu einem zentralen Thema auf Vorstandsebene. Sie entwickelt sich schnell von einem sentimentalen oder protektionistischen Hype zu einer strategischen Notwendigkeit. Laut einer Studie von IDC hat Datensouveränität Wachstum und Innovation als strategische Priorität inzwischen bei jeder vierten Organisation überholt.

Absolute digitale Souveränität und Kontrolle zu erreichen, ist eine mehrjährige Reise und zugleich eine überwältigende sowie disruptive Aufgabe. Für die meisten Unternehmen ist die richtige Datenlokation der erste realistische Ausgangspunkt. Zu steuern, wo Daten liegen, ist eine notwendige Voraussetzung für Souveränität. Ihr eigentlicher Vorteil besteht darin, dass sie alle anderen Ebenen erst ermöglicht: Verschlüsselung, Zugriffssteuerung, Audit-Compliance, Portabilität und unabhängig Recovery beruhen alle auf einer darunter liegenden, kontrollierten und dokumentierten

AUF EINEN BLICK

WICHTIGE KENNZAHLEN

Bis 2028 werden 60 % der Organisationen aufgrund geopolitischer Unsicherheiten sensible Workloads in neue Cloud-Umgebungen migrieren, um ihre Anforderungen an digitale Souveränität zu erfüllen, Risiken zu reduzieren und ihre Autonomie zu erhöhen

WORAUF ES ANKOMMT

Eine ausgereifte und intensiviertere Hybrid-Cloud- und Multicloud-Strategie betrachtet Souveränität als mehrschichtiges Betriebsmodell, das auf den Säulen Resilienz, Kontrolle, Portabilität und kommerzieller Wahlfreiheit basiert. Sie stellt somit das genaue Gegenteil einer starren,

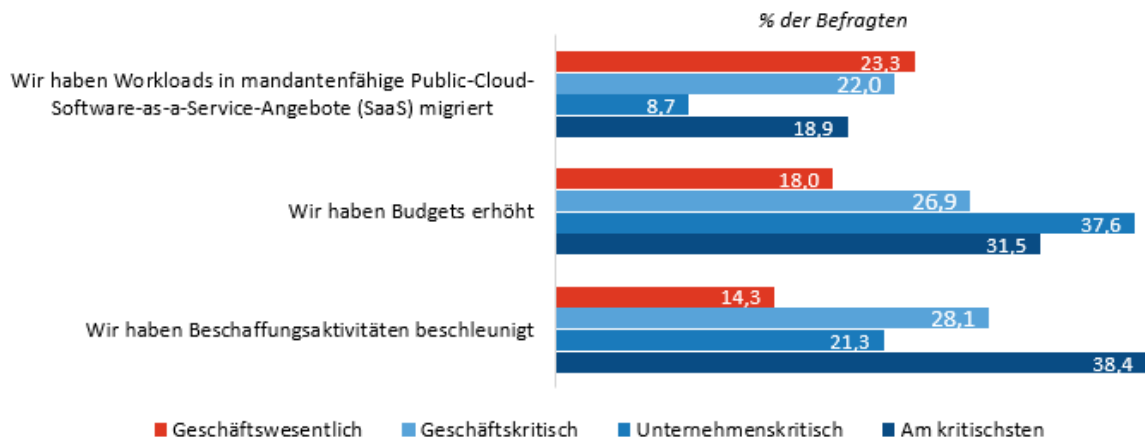
Ebene der Datenresidenz. So bildet sie die Grundlage für die Einhaltung gesetzlicher Vorschriften. Im Kern drehen sich die DSGVO, der EU Data Act, die NIS2-Richtlinie und die meisten nationalen Rahmenwerke darum, wo Daten verarbeitet und gespeichert werden und welchem Recht sie unterliegen. Sie ermöglicht zudem direkte Audit-Trails, dokumentierte Zugriffskontrollen sowie Nachweise zur Herkunft und Nachvollziehbarkeit von Daten, wie sie von Regulierungsbehörden zunehmend verlangt werden.

IDC ist der Ansicht, dass Datenlokalität – also die Fähigkeit, festzulegen, wo Daten physisch gespeichert sind – die am besten umsetzbare Dimension von Souveränität ist und jene, die Organisationen am direktesten kontrollieren können. Viele betrachten dies als zentrale Säule des Enterprise Risk Management und der Wettbewerbsstrategie. Angesichts der sich weiter verschärfenden geopolitischen Unsicherheiten legen Unternehmen zunehmend den Schwerpunkt auf folgende Prioritäten: Laut IDC FutureScape: Worldwide Cloud 2026 Predictions (IDC #US53859425, Oktober 2025) werden bis 2028 60 % der Organisationen mit Anforderungen an digitale Souveränität sensible Workloads in neue Cloud-Umgebungen migrieren, um Risiken zu reduzieren und ihre Autonomie zu erhöhen.

Organisationen in EMEA haben bereits begonnen, die Grundlagen dafür zu schaffen. Laut der IDC-Umfrage *CloudOps and Governance* vom Dezember 2025 erhöhen 69 % der Organisationen ihre Budgets für Data Governance, Souveränität, Sicherheit und Resilienz im Jahr 2026. Es gibt keinen massenhaften Cloud-Ausstieg und keine Kehrtwende weg von der Cloud. Tatsächlich geben nur 23 % der Organisationen an, Daten aus der Cloud zurückzuführen. Eine größere Zahl von Organisationen hat andere Maßnahmen ergriffen: Sie haben eine Dateninventarisierung und -klassifizierung abgeschlossen, Budgets und Teams für das Souveränitäts-, Risiko- und Resilienzmanagement aufgebaut sowie ein besseres Verständnis für die geteilten Verantwortlichkeiten in der Cloud entwickelt. Wie Abbildung 1 zeigt, haben bei den kritischsten Workloads 38 % der Organisationen Beschaffungsaktivitäten für Infrastruktur beschleunigt, um Risiken zu mindern, und 32 % haben ihre Budgets erhöht. Im Vergleich dazu setzen bei geschäftswesentlichen Workloads mehr Organisationen auf mandantenfähige Umgebungen.

Dies steht für eine ausgereifte und intensiviertere Hybrid-Cloud- und Multicloud-Strategie: eine Strategie, die Souveränität als mehrschichtiges Betriebsmodell versteht, das auf Resilienz, Kontrolle, Portabilität und kommerzieller Wahlfreiheit basiert. Diese Strategie lehnt eine starre, absolutistische Forderung nach Datenisolation im Rahmen einer On-Premises-Strategie ab, da dies voraussichtlich zu Problemen wie mangelnder Skalierbarkeit und Geschwindigkeit, hohen CapEx-Investitionen und eingeschränktem Zugang zu Cloud-Innovationen führen würde.

Unternehmen in der EMEA-Region wenden sich von theoretischer Reinheit in Bezug auf Souveränität ab und wenden sich stattdessen einem architekturorientierten Pragmatismus zu. Das bedeutet, Datensouveränität nicht als Zielzustand zu betrachten, sondern als fortlaufende Disziplin, die in die Infrastruktur integriert werden muss.

ABBILDUNG 1: **Reaktion von Organisationen in EMEA auf Geschäftsrisiken je Workload-Kategorie**

n = 509

Quelle: IDC-Umfrage CloudOps and Governance, Dezember 2025

Zusammenfassend ist IDC der Ansicht, dass sich Organisationen in EMEA von theoretischer Reinheit bei Souveränität entfernen und hin zu architekturgetriebenem Pragmatismus bewegen. Das bedeutet, Datensouveränität nicht als Zielzustand zu betrachten, sondern als fortlaufende Disziplin, die in die Infrastruktur integriert werden muss. Ziel ist es, Risiken zu reduzieren und gleichzeitig Innovation, Flexibilität und Geschwindigkeit zu bewahren. Cloud-Storage spielt als unabhängige, auf Souveränität vorbereitete Schicht eine zentrale Rolle dabei.

Definitionen

Wenn sie nicht in den Geschäftsergebnissen verankert wird, droht Souveränität zu abstrakt und nicht handlungsorientiert zu werden. Digitale Souveränität ist mehrschichtig. Sie umfasst die Fähigkeit einer Organisation oder eines Staates, die eigenen digitalen Assets, die eigene Infrastruktur sowie die eigenen Fähigkeiten frei von externer Einflussnahme zu steuern. Innerhalb dieses Rahmens bildet die Datensouveränität den grundlegenden Ausgangspunkt. Sie umfasst die Fähigkeit, zu steuern, wo Daten gespeichert sind, welche Gesetze auf sie Anwendung finden, wer darauf zugreifen kann und wie sie geschützt und wiederhergestellt werden können. Andere Dimensionen, wie KI-Souveränität, Kompetenzsouveränität oder operative Souveränität, hängen davon ab, die Datensouveränität richtig umzusetzen.

Die zentralen Dimensionen zur Umsetzung der Prinzipien der Datensouveränität sind in Tabelle 1 aufgeführt. Zusammen bilden sie ein praktisches Betriebsmodell, mit dem Organisationen ihren aktuellen Reifegrad bewerten und Investitionen priorisieren können.

TABELLE 1: **Die vier Dimensionen der Datensouveränität: Definitionen, Anforderungen und Cloud-Funktionen**

DIMENSIONEN	DEFINITIONEN	WICHTIGE ANFORDERUNGEN	WORAUF BEI CLOUD-FUNKTIONEN ZU ACHTEN IST
Daten	Regelt, wo Daten physisch gespeichert sind und wer darauf zugreifen kann	Datenresidenz, Verschlüsselung, Zugriffskontrolle	Auswahl regionaler Rechenzentren in EU/EMEA; kundenseitig verwaltete Verschlüsselungsschlüssel; Replikation; granulare Zugriffsrichtlinien
Rechtlich	Bestimmt, welche Rechtsordnung für Daten gilt und wer über Override-Befugnisse verfügt	Klare Jurisdiktion, Vertragsbedingungen, Risiko von Herausgabeanordnungen	Kundenseitige Wahl, wo Daten gespeichert werden
Operativ	Stellt Kontinuität und Recovery sicher, selbst wenn ein primärer Anbieter ausfällt	Sicherheit, Datenresilienz, Flexibilität und Industriestandards	Immutable und unsichtbarer Object Storage; WORM-Compliance; Replikation; nahtlose Backup-/Recovery-Integration
Technisch	Bewahrt die Fähigkeit, Daten ohne Vendor-Abhängigkeit zu verschieben, wiederherzustellen und eine Umgebung zu verlassen	Immutability, Datenportabilität oder Exit Readiness	S3-kompatible API für Multicloud-Portabilität; keine Egress-Gebühren; Skalierbarkeit und Flexibilität über Hybrid-Architekturen hinweg; vertragliche Transparenz bei Datenmigration

Quelle: IDC, 2026

Souveränität ist keine Produktkategorie. Sie ist das Ergebnis von Governance-, Architektur- und Betriebsentscheidungen. Kein einzelner Vendor bietet End-to-End-Souveränität. Doch jede Ebene des Technology Stacks – beginnend mit der Datenspeicherung – wirkt entweder als Einschränkung oder als Enabler für die darüberliegenden Ebenen. Führungskräfte sollten drei Fragen beantworten können:

- » Können Sie Ihre sensiblen Daten kontrollieren? (Haben Sie Flexibilität und Wahlmöglichkeiten bei Standorten, Datentransparenz und Portabilität?)
- » Können Sie die Daten unabhängig verwalten, sichern und steuern? (Haben Sie Kontrolle über Sicherheit, Richtlinien, Datenresidenz und Verschlüsselung?)
- » Können Sie die Daten verschieben, wenn sich die Rahmenbedingungen ändern? (Ist die Umgebung interoperabel, portabel und transparent?)

Vorteile

Bei guter Umsetzung geht Datensouveränität über einfache Compliance hinaus und führt zu einer vertrauenswürdigen, robusten und resilienten Datenarchitektur. IDC empfiehlt Organisationen, den Fokus von angstgetriebener Compliance hin zu einem strategischen Vorteil zu verschieben. Ein resilienz- und autonomieorientierter Ansatz für Souveränität liefert relevante Vorteile in den folgenden fünf Dimensionen:

- » **Geringere geopolitische und rechtliche Risiken:** Organisationen, die eine klare Datenresidenz nachweisen können, sind besser in der Lage, Anforderungen an den Datenstandort zu dokumentieren und gegebenenfalls

durchzusetzen, was in Diskussionen über Souveränität ein wichtiges Instrument zur Risikominderung darstellt. Auch wenn der Datenstandort allein keine jurisdiktionellen Risiken oder Probleme bei der grenzüberschreitenden Durchsetzung neutralisiert, so bietet er doch eine dokumentierte und auditierbare Grundlage. Da sich das regulatorische Umfeld in EMEA weiterentwickelt – mit DSGVO, NIS2, dem EU Data Act und einer wachsenden Zahl nationaler Rahmenwerke, die neue Anforderungen an das Datenmanagement stellen –, wird der Nachweis, wo Daten liegen und wie sie verwaltet werden, zur grundlegenden Erwartung.

- » **Höhere Resilienz und Kontinuität:** Eine auf Souveränität ausgerichtete Architektur ist von ihrer Konzeption her widerstandsfähiger. Unternehmen, die ihre Datenspeicherung auf unabhängige Anbieter verteilen, statt sie in einer einzigen Hyperscale-Umgebung zu konzentrieren, verringern den Auswirkungsbereich eines einzelnen Ausfallpunkts. Immutable, geografisch verteilte Datenspeicherung ist eine Voraussetzung für Business Continuity.
- » **Bessere operative Kontrolle:** Unabhängige Ebenen für die Datenspeicherung und -verwaltung ermöglichen es Unternehmen, Zugriffsrichtlinien, die Verwaltung von Verschlüsselungsschlüsseln und Entscheidungen zum Datenlebenszyklus sinnvoll zu steuern. Diese operative Kontrolle ist besonders wertvoll für Branchen, die regulatorischen Vorgaben unterliegen und in denen dokumentierte Audit-Trails, Aufbewahrungsfristen sowie die Fähigkeit, nachzuweisen, dass Daten nicht unbefugt abgerufen oder verändert wurden, erforderlich sind.
- » **Wirtschaftliche Widerstandsfähigkeit:** Die Konzentration auf nur einen einzigen Lieferanten birgt geschäftliche Risiken. Organisationen, die ihre Datenlandschaft um einen einzigen Hyperscale-Anbieter aufgebaut haben, sehen sich mit asymmetrischen Verhandlungsdynamiken konfrontiert: Sie müssen mit hohen Egress-Kosten, restriktiven Vertragsbedingungen sowie begrenzter Verhandlungsmacht bei Preisänderungen oder Serviceunterbrechungen rechnen. Souveräne Architektur, die sich durch Portabilität, Interoperabilität und unabhängige Storage-Schichten auszeichnet, stellt das kommerzielle Gleichgewicht wieder her und schützt Organisationen vor Lock-in, während die Preise und Richtlinien für die Cloud zunehmend umkämpft sind.
- » **Mehr Spielraum für Innovation:** Paradoxe Weise schafft eine starke Souveränitätsposition mehr Raum für Innovationen, nicht weniger. Vertrauen in Daten ist die Voraussetzung für eine erfolgreiche Einführung von KI, die Entwicklung von Datenprodukten und eine grenzüberschreitende Zusammenarbeit mit Daten. Organisationen, die ihrer Datenkontrolle und Resilienz vertrauen, können Ressourcen von der reaktiven Problembewältigung hin zu Innovation und Differenzierung im Wettbewerb verlagern.

Trends

Digitale Souveränität ist in der Mainstream-Enterprise-IT-Strategie angekommen. Dies ist auf eine Kombination aus regulatorischem Druck, geopolitischer Instabilität und Abhängigkeitsrisiken durch die Konzentration auf eine einzige Cloud zurückzuführen. Laut IDC werden CIOs multinationaler Unternehmen ihre Investitionen in modulare, souveränitätsfähige Cloud- und Datenlokalisierungsumgebungen bis 2028 um 65 % erhöhen, um den Betrieb angesichts steigender Souveränitätsanforderungen zukunftssicher zu gestalten.

Für multinationale Unternehmen mit Aktivitäten in EMEA hat sich die Risikobewertung deutlich verändert: Die Möglichkeit plötzlicher regulatorischer Änderungen, Sanktionen oder Zugriffsbeschränkungen ist angesichts der aktuellen geopolitischen Entwicklungen nicht mehr theoretisch.

Trotz dieser Dringlichkeit herrscht am Markt nur begrenzt Klarheit darüber, was Souveränität im digitalen Betrieb tatsächlich verlangt. Organisationen entwickeln ein breites Spektrum an Antworten, das von pragmatischen Architekturentscheidungen bis hin zu Überkorrekturen reicht. Dabei verwechseln sie reine Standortkontrollen mit vollständiger digitaler Souveränität. Deshalb ist es entscheidend, Klarheit darüber zu haben, was Souveränität ist – und vor allem, was sie nicht sein sollte.

Was Souveränität NICHT ist

IDC beobachtet, dass sich der EMEA-Markt als Reaktion auf Datensouveränität nicht in Richtung Cloud-Repatriierung bewegt.

In wettbewerbsintensiven Branchen wie dem Bank- und Finanzdienstleistungssektor im Vereinigten Königreich führt ein starker Fokus auf KI-getriebene Innovation in Kombination mit ausgereiften, bestehenden Ansätzen für Risikomanagement und Compliance dazu, dass Organisationen einen risikobasierten und praktischen Ansatz für Souveränität wählen.

Eine vollständige Rückkehr zu On-Premises-Infrastrukturen würde die Agilität, Wirtschaftlichkeit und Skalierbarkeit opfern, die moderne Organisationen benötigen. IDC beobachtet stattdessen einen Markt, der sich hin zu souveränen Architekturmustern bewegt. Diese basieren auf Hybrid-Cloud-, Multicloud- und verteilten Storage-Landschaften und ermöglichen Flexibilität, Interoperabilität und Standortwahl, ohne die Wirtschaftlichkeit der Cloud aufzugeben.

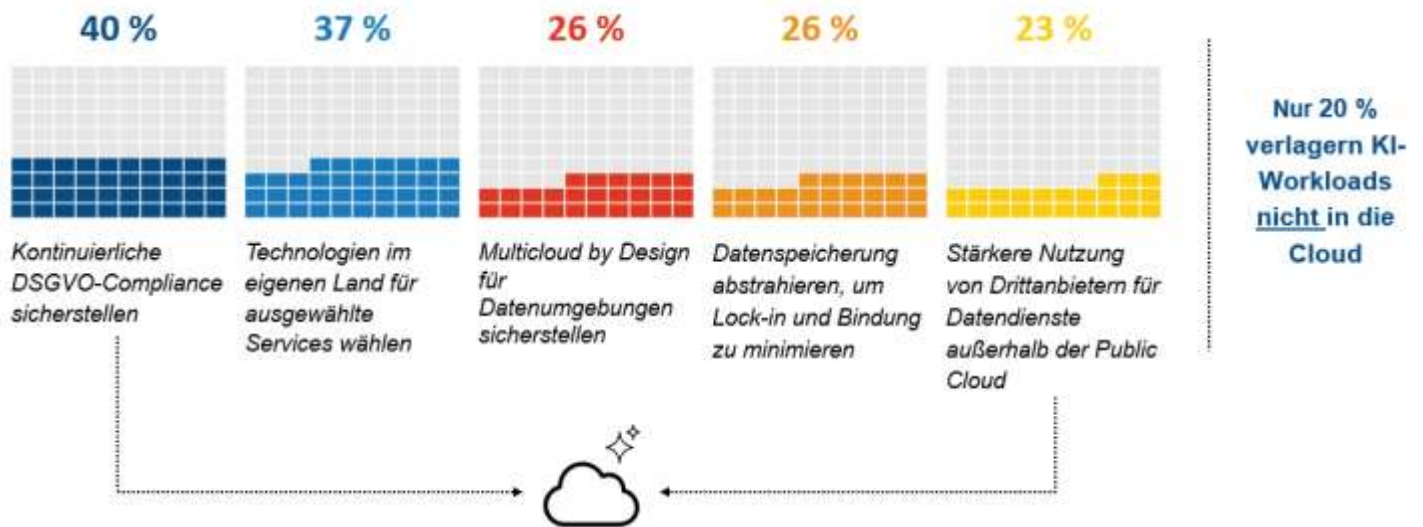
Laut der im März 2026 durchgeführten IDC-Umfrage *FERS*, die die Auswirkungen des Kriegs im Nahen Osten auf IT-Trends untersucht, priorisieren 35 % der digital-nativen Organisationen in den nächsten 6 bis 12 Monaten Investitionen in Cloud- und Rechenzentrumsresilienz durch mehrere Availability Zones und Regionen. Nur 18 % investieren hingegen in souveräne oder lokal betriebene Rechenzentren. Dies bestätigt noch einmal, dass eine massenhafte Rückverlagerung nicht als praktische Antwort auf wachsende Souveränitätsbedenken betrachtet wird.

Darüber hinaus nannten 44 % der Digital Natives die Strategie „Supplier Diversification“ für die IT-Architektur im Zusammenhang mit dem Krieg im Nahen Osten, während sich 20 % für lokale souveräne Rechenzentren entschieden.

Es gibt zudem eine deutliche Divergenz zwischen Digital Natives und Digital Followers. Digital-native Organisationen gehen Souveränität tendenziell pragmatisch an und konzentrieren sich auf Resilienz und operative Autonomie. Unter den Digital Followers gibt es einen höheren Anteil, der zu standortbezogenen Richtlinien oder EU-Vendor-only-Ansätzen tendiert, ohne dass damit eine verhältnismäßige Risikoreduktion verbunden ist. IDC ist der Ansicht, dass die nächste Phase der Souveränität in EMEA durch Designentscheidungen gewonnen wird, die Wahlfreiheit erhalten, statt durch Entweder-oder-Beschränkungen.

Laut IDC stehen IT-Teams unter Druck, Resilienz innerhalb vorgegebener Budgets sicherzustellen. Dadurch bleibt die Cloud für Storage- und Archivierungszwecke weiterhin sehr attraktiv.

Nach der Datenklassifizierung verfolgen Organisationen einen differenzierten Ansatz zur Risikominderung und implementieren je nach Risikoprofil geeignete technische Maßnahmen, wie in Abbildung 2 dargestellt.

ABBILDUNG 2: **Technische Mechanismen zur Adressierung von Datensouveränitätsbedenken**

n = 509

Quelle: IDC-Umfrage CloudOps and Governance, Dezember 2025

Portabilität wird zu einem Designprinzip

Bis 2027 werden 70 % der G5000 ihre Kern-Workloads so umgestalten, dass sie über private und öffentliche Cloud-Umgebungen hinweg portabel sind. Damit reagieren sie auf Resilienz-, KI- und Datenschutzvorschriften. Organisationen bewerten ihre Cloud-Storage- und Infrastrukturpartner nicht mehr nur nach deren aktuellen Fähigkeiten, sondern auch danach, wie gut sie Exit-Readiness und Mobilität über unterschiedliche Umgebungen hinweg unterstützen. Portabilität ist kein neues Konzept und bleibt zwar ein architektonisches Ziel, ist operativ jedoch schwer umzusetzen. Historisch gesehen waren Workloads mit starker Data Gravity, die eng an proprietäre Hyperscale-APIs gekoppelt sind, mit kostspieligen und disruptiven Workload-Migrationen verbunden. Zu den wichtigsten Enablern zählen standardisierte Object-Storage-APIs, insbesondere S3-kompatible Schnittstellen, moderne Backup- und Datenmanagementarchitekturen, die Daten von Compute entkoppeln, sowie ein bewusster Architekturwechsel, bei dem Storage als unabhängige, austauschbare Schicht implementiert wird.

Diese architektonische Flexibilität gibt Organisationen letztlich mehr Kontrolle darüber, wo Daten liegen, wie sie sich bewegen und welche Rechtsräume und Anbieter den Zugriff darauf bestimmen. Dadurch werden Datenlokalität und Strategien für digitale Souveränität gestärkt.

Metadatenkontrolle gewinnt strategisch an Bedeutung

Die Kontrolle über die Platzierung von Metadaten, Kopiedaten und Archivdaten wird zu einem entscheidenden Bestandteil der Business-Continuity-Strategie. Da die regulatorischen Anforderungen an die Datenaufbewahrung, die Audit-Trails und die Wiederherstellung zunehmen, ist die Fähigkeit entscheidend, den vollständigen Datenlebenszyklus – einschließlich sekundärer Kopien und Langzeitarchive – in einer kompatiblen, aber getrennten Speicherumgebung zu verwalten.

Erwägungen zu Wasabi

Das Argument, Storage in den Mittelpunkt jeder praktischen Souveränitätsstrategie zu stellen, ist einfach: Storage ist der Ort, an dem Kontrolle, Aufbewahrung, Immutability und Recovery-Fähigkeit Realität werden. Abstrakte Souveränitätsversprechen sind wertlos, wenn die zugrunde liegenden Daten von einem Dritten außerhalb des Governance-Rahmens der Organisation abgerufen, verändert, verschoben oder gesperrt werden können. Die Auswahl einer unabhängigen Object-Storage-Schicht, die IT-Teams dabei unterstützt, die vier Dimensionen der Datensouveränität zu adressieren, ist eine der wirkungsvollsten Architekturentscheidungen, die eine Organisation in EMEA treffen kann.

Warum Storage für praktische Souveränität zentral ist

Eine unabhängige Storage-Ebene, die architektonisch von der primären Compute-Umgebung entkoppelt ist, schafft einen relevanten Souveränitätspuffer, ohne dabei die Wirtschaftlichkeit der Cloud oder die operative Agilität zu beeinträchtigen. Hyperscale-Cloud-Anbieter überzeugen durch ihre Wirtschaftlichkeit und Fähigkeiten, bergen aber auch Konzentrationsrisiken. Werden Storage-, Compute-, Netzwerk- und Anwendungsservices von einem einzigen Anbieter bezogen, wird die Souveränitätsposition der Organisation durch dessen juristische Ausrichtung, Vertragsbedingungen und Zusagen zur Business Continuity eingeschränkt.

Wie Wasabi EMEA-Anforderungen an Souveränität adressiert

Wasabi ist ein unabhängiger Anbieter von Cloud Object Storage und positioniert sich als leistungsstarke und kosteneffiziente Alternative zu Hyperscale-Storage-Services. Wasabi erfüllt im Kontext der Datensouveränität in EMEA mehrere der in diesem Dokument identifizierten praktischen Souveränitätsanforderungen, darunter:

- » **Wahl der regionalen Bereitstellung:** Wasabi betreibt Storage-Regionen in EMEA, darunter Standorte in Amsterdam, Frankfurt, London, Paris und Mailand. So können Organisationen ihre Anforderungen an die Datenresidenz durchsetzen, ohne auf cloud-native Storage-Funktionen verzichten zu müssen.
- » **Unabhängige Object-Storage-Schicht:** Die S3-kompatible API von Wasabi ermöglicht es Organisationen, den Storage des Unternehmens in bestehende Workflows, Backup-Lösungen und Multicloud-Architekturen zu integrieren, ohne neue Abhängigkeiten von einem einzelnen Anbieter zu schaffen. Dies ist die praktische Grundlage des Prinzips Portability by Design.
- » **Immutable und unsichtbarer Storage:** Wasabi unterstützt WORM-Object-Storage (write once, read many) für regulatorische Compliance und Ransomware-Resilienz. Die Covert Copy-Funktion ist eine neue Innovation, die versteckte, manipulationsresistente sekundäre Kopien kritischer Daten ermöglicht. Dadurch wird dieser Schutz erweitert und es wird sichergestellt, dass Backup-Daten für die Wiederherstellung zugänglich bleiben, selbst wenn primäre Kopien kompromittiert oder gelöscht werden.
- » **Hybrid-Cloud- und Multicloud-Kompatibilität:** Wasabi ist nativ in führenden Backup-, Recovery- und Datenmanagementplattformen integriert und ermöglicht es Organisationen, souveräne Storage-Schichten in Hybrid-Cloud- und Multicloud-Architekturen aufzubauen – ganz ohne kostspieliges Reengineering.

Wasabi mit dem Souveränitätsrahmen verbinden

Gemessen am in Tabelle 1 eingeführten Vier-Linsen-Rahmen für Souveränität bietet Wasabi:

- » **Datenkontrolle:** Wasabi hilft dabei, Richtlinien zur Speicherung von Daten durchzusetzen – mit regionaler Auswahl, rollenbasierten Zugriffskontrollen und richtliniengesteuertem Access Management.
- » **Operative Autonomie:** Wasabi bietet eine Governance-Schicht für Backup, Recovery und Datenlebenszyklusmanagement, die unabhängig von primären Hyperscale-Umgebungen ist.
- » **Technische Resilienz:** Die Funktionen Immutability, Covert Copy, Multi-User Authorization und WORM schützen vor Ransomware, versehentlichem Löschen und böswilligen Eingriffen.
- » **Strategische Autonomie:** Das S3-kompatible Modell von Wasabi ohne Egress-Gebühren ermöglicht Skalierbarkeit und Flexibilität, verbessert die Exit-Readiness, reduziert Lock-in-Effekte und bewahrt die kommerzielle Verhandlungsmacht über verschiedene Umgebungen hinweg.

Herausforderungen und Überlegungen für Führungskräfte

Kein einzelner Anbieter bietet End-to-End-Souveränität. Storage ist einer der wichtigsten praktischen Hebel, um Souveränitätsergebnisse zu erreichen. Allein reicht er jedoch nicht aus. Die Ergebnisse hängen ebenfalls von der Datenklassifizierung, der Verschlüsselungs- und Key-Management-Strategie, dem Richtliniendesign, der Risiko-Governance sowie den Architekturentscheidungen für die gesamte Datenlandschaft ab. Wasabi sollte nicht als schlüsselfertige Souveränitätslösung, sondern als Bestandteil einer souveränen Architektur bewertet werden.

Zudem ist Wasabi ein Unternehmen mit Hauptsitz in den Vereinigten Staaten. Dies ist für einige Käufer in EMEA ein wichtiger Aspekt, insbesondere im öffentlichen Sektor und in Rechtsräumen, in denen Beschaffungsrahmen zunehmend in der EU registrierte Anbieter, lokale Abrechnungseinheiten oder länderspezifische Supportmodelle verlangen. Obwohl Wasabi Rechenzentren innerhalb der EU betreibt und Daten nach geltendem lokalen Recht speichert, empfiehlt IDC Käufern mit den strengsten Souveränitätsanforderungen – einschließlich solcher, die eine EU-Unternehmensregistrierung oder nationale Herkunftsnachweise erfordern – eine detaillierte Due Diligence, um zu bewerten, ob die aktuelle Betriebsstruktur von Wasabi ihre spezifischen Anforderungen erfüllt. IDC empfiehlt Organisationen, diese Dimension ausdrücklich als Teil ihrer Vendor-Bewertung zu prüfen, statt davon auszugehen, dass der geografische Standort der Daten ausreicht, um alle Souveränitätsanforderungen zu erfüllen.

Gleichzeitig setzen versierte Organisationen, die Innovation, Resilienz und Souveränität in Einklang bringen, in Gesprächen mit IDC auf folgende Strategien, um alle Stakeholder mitzunehmen:

- » **Die Frage neu formulieren:** Der Unternehmenssitz und die operative Datenkontrolle sind zwei verschiedene Dinge. Nur Letztere beeinflusst die Souveränitätsposition wesentlich.
- » **Den CLOUD Act einordnen:** Auch wenn das Risiko real ist, verstehen versierte Organisationen, dass es möglicherweise überschätzt wird. Kundenseitig verwaltete Verschlüsselungsschlüssel sind eine starke Möglichkeit, um diese Herausforderungen zu mindern.
- » **EU-Anbieter validieren:** Es ist wichtig, zu prüfen, ob einige in der EU registrierte Anbieter mit US-Unternehmen als Unterauftragsverarbeiter zusammenarbeiten. Denn eine Unternehmenshülle ist nicht gleichbedeutend mit absoluter Souveränität. Eine vollständige Bill-of-Materials-Analyse kann Supply-Chain-Risiken aufdecken und zeigen, dass sich nicht alle Risiken vollständig mindern lassen.

- » **Branchenanforderungen verstehen:** Nicht alle Unternehmen benötigen für alle Daten und Workloads dieselbe Due Diligence wie Käufer aus den Bereichen Verteidigung, Nachrichtendienste und kritische nationale Infrastruktur, die harten regulatorischen Vorgaben unterliegen.
- » **Breite Compliance:** Versierte Organisationen prüfen grundlegende Aspekte, etwa ob diversifizierte Cloud-Anbieter Vorschriften wie die DSGVO unterstützen und über Zertifizierungen und Kontrollen wie SOC 2 und ISO 27001 für ihre Rechenzentrumsbereitstellungen und Storage-Umgebung verfügen.

Wasabi hat Einfühlungsvermögen und Verständnis für die Souveränitätsbestrebungen der EMEA-Region bewiesen. Das starke EMEA-Führungsteam von Wasabi beeinflusst die Engineering-Roadmap. Das Unternehmen arbeitet mit seinen Channel-Partnern daran, die Anforderungen an souveräne Daten in ganz EMEA zu erfüllen, und investiert aktiv in Rechenzentren in Europa (Amsterdam, Paris, Frankfurt, Mailand und im Vereinigten Königreich) sowie in Engineering-Funktionen, die den Kunden mehr Kontrolle über ihre Daten und erweiterte Sicherheitsfunktionen bieten.

Wasabi muss seine Präsenz in der EMEA-Region weiter ausbauen, seine Kompetenzen im Bereich Data Governance stärken und auf die Bedenken der Käufer hinsichtlich der Herkunft von Daten eingehen, denen Fragen der Souveränität besonders am Herzen liegen. Das Unternehmen verfügt über ein erhebliches und wachsendes Marktpotenzial. Zudem sollte das Unternehmen eine „Better Together“-Strategie mit einem Anbieter für Data Protection in Betracht ziehen, um alle Grundlagen souveräner Datendienste abzudecken. Schließlich sollte das Unternehmen seine Compliance mit Datenregulierungen in EMEA sowie seine Sicherheitszertifizierungen hervorheben.

Angesichts des massiven Sovereignty-Washings in der Branche sollte Wasabi das Thema nicht überdrehen, sondern sich auf andere starke Geschäftsergebnisse konzentrieren, die das Unternehmen liefert. Dazu zählen etwa die einfache Nutzung, die starke Cloud-Wirtschaftlichkeit und die Kundenfreundlichkeit.

Fazit

Organisationen in EMEA, die Souveränität als reine Compliance-Checkbox behandeln, werden immer wieder überrascht werden. Organisationen, die dies als grundlegendes Designprinzip betrachten, schaffen das Vertrauen, die Resilienz und die operative Kontrolle, die für ein datengetriebenes Unternehmen erforderlich sind.

Die Dringlichkeit, Risiken bei der Datenkontrolle zu mindern, hat durch den Aufstieg von KI zugenommen. Ohne angemessene Datenresidenz, Governance und Recovery-Fähigkeit fehlt Organisationen die Grundlage für den verantwortungsvollen Einsatz von KI.

Der richtige Weg besteht weder darin, theoretische Reinheit anzustreben, noch ausschließlich IT-Anbieter aus dem eigenen Land einzusetzen. Es geht darum, eine Reihe kleiner, aber klarer operativer Entscheidungen zu treffen: Wo werden Daten gespeichert? Wie werden sie verwaltet? Wie werden sie wiederhergestellt? Wie portabel sind sie? Zusammen schaffen diese Entscheidungen eine Souveränitätsposition, die resilient, pragmatisch und kommerziell tragfähig ist.

IDC-Empfehlungen für C-Level-Führungskräfte in EMEA

- » **Den Blick auf Souveränität verändern:** Betrachten Sie Datensouveränität nicht nur als Compliance-Verpflichtung, sondern als Resilienzmechanismus, der Störungen minimiert und Vertrauen für datengetriebene Innovationen schafft.

- » **Der Versuchung widerstehen, sich ausschließlich auf EU-basierte Anbieter zu beschränken:** Globale Cloud-Anbieter und Storage-Unternehmen sind etabliert, angesehen und verfolgen langfristige, globale Ambitionen. Sie erkennen zudem differenzierte regionale Anforderungen und entwickeln Mechanismen, um ihre regionalen Kunden bei der Einhaltung von Souveränitätsprinzipien zu unterstützen. Eine Risikoanalyse, die untersucht, inwieweit die Auslösung des CLOUD Act möglicherweise überbewertet wird und welcher Anteil der IT-Assets tatsächlich gefährdet ist, kann dabei helfen, das Souveränitätsargument in praktische geschäftliche Begriffe zu übersetzen. Dadurch entsteht mehr Klarheit, sodass Innovation und Resilienz ausbalanciert werden können.
- » **Daten klassifizieren und differenzierte Kontrollen anwenden:** Nicht alle Daten müssen auf die gleiche Weise aufbereitet werden. Identifizieren Sie sensible, regulierte und geschäftskritische Datensätze und wenden Sie entsprechend mehrschichtige Kontrollen an.
- » **Unabhängige Recovery und operative Resilienz aufbauen:** Stellen Sie sicher, dass Backup- und Recovery-Architekturen von primären Cloud-Anbietern entkoppelt sind. Immutabler, externer Object Storage ist eine kritische Schutzmaßnahme.
- » **Portabilität und Verhandlungsmacht bewahren:** Vermeiden Sie tiefen Vendor Lock-in. Entwerfen Sie Ihre Hybrid-Cloud- und Multicloud-Umgebung unter Berücksichtigung von Exit Readiness und Interoperabilität.
- » **Mehrere Stakeholder einbeziehen:** Souveränität umfasst Recht, IT, Sicherheit, Compliance und das Business. Governance-Rahmenwerke müssen diese Breite widerspiegeln.
- » **Datensouveränität auf KI-Resilienz ausrichten:** Mit der zunehmenden Verbreitung von KI-Workloads wird souveräne Dateninfrastruktur zur Grundlage für konforme und vertrauenswürdige KI.

Über die Analystin



Archana Venkatraman, Senior Research Director, Cloud Data Management

Archana Venkatraman leitet IDC Research zu European CloudOps and Governance sowie zu Cloud Data Management. Im Rahmen des CloudOps-Schwerpunkts analysiert Archana Multicloud-Management und -Betrieb, Cloud Economics und FinOps, Observability, Cloud-Konsolidierung sowie Cloud Governance und Kontrolle. Ein großer Schwerpunkt ihrer Forschung liegt auf den Themen Cloud Value Realization, Cloud-Native-Success und Operational Excellence.

HINWEIS DES SPONSORS

Wasabi ermöglicht es Organisationen durch sein Engagement für Transparenz, Verantwortlichkeit und Cyber-Resilienz, kritische Daten sicher zu speichern, zu verwalten und wiederherzustellen. Gleichzeitig werden Compliance vereinfacht und operative Risiken reduziert.

Auf Basis eines Defense-in-Depth-Sicherheitsmodells schützt Wasabi Kundendaten durch Verschlüsselung im Ruhezustand und während der Übertragung, MFA- und SSO-fähige Zugriffskontrollen, immutable Object-Lock-Storage und Covert Copy® Virtual-Air-Gapping-Technologie für erhöhte Ransomware-Resilienz. Darüber hinaus wird die Wasabi-Infrastruktur in sicheren, redundanten Rechenzentren gehostet, die nach SOC 2, ISO 27001 und PCI-DSS zertifiziert sind.

Wasabi unterstützt wichtige regulatorische und branchenspezifische Rahmenwerke wie HIPAA, DSGVO, CJIS, FERPA, SEC/FINRA und die Anforderungen der CFTC.

Weitere Informationen finden Sie im [Wasabi Trust Center](#)



Der Inhalt dieses Dokuments wurde aus vorhandenen Studien übernommen, die auf www.idc.com veröffentlicht wurden.

IDC Research, Inc.

One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

Diese Publikation wurde von IDC Custom Solutions erstellt. Die hier dargestellten Meinungen, Analysen und Forschungsergebnisse stammen aus detaillierteren Studien und Analysen, die von IDC unabhängig durchgeführt und veröffentlicht wurden, sofern nicht ausdrücklich auf eine Sponsoring-Partnerschaft mit einem bestimmten Anbieter hingewiesen wird. IDC Custom Solutions stellt IDC-Inhalte in einer Vielzahl von Formaten zur Verfügung, damit sie von unterschiedlichen Unternehmen verbreitet werden können. Dieses IDC-Material ist für den externen Gebrauch lizenziert. Die Verwendung bzw. Veröffentlichung dieser IDC-Studie bedeutet in keiner Weise, dass IDC die Produkte oder Strategien des Sponsors oder Lizenznehmers befürwortet.

Die International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktanalysen, Beratungsdienstleistungen und Veranstaltungen für die Bereiche Informationstechnologie, Telekommunikation und Verbrauchertechnologie. Mit weltweit mehr als 1.300 Analysten bietet IDC globale, regionale und lokale Expertise zu Technologie- und Branchenchancen sowie Trends in über 110 Ländern. Die Analysen und Erkenntnisse von IDC helfen IT-Fachleuten, Führungskräften und Mitgliedern der Investment-Community dabei, fundierte Technologieentscheidungen zu treffen und wesentliche Geschäftsziele zu erreichen.

©2026 IDC. Die Vervielfältigung ohne entsprechende Genehmigung ist untersagt. Alle Rechte vorbehalten. [CCPA](#)