

DATENSOUVERÄNITÄT IN EUROPA



In der Vergangenheit war Datensouveränität vor allem ein Spezialthema – ein Punkt, der in Auswahlverfahren für Technologieanbieter eher weiter unten auf der Liste stand. In einigen Marktsegmenten war sie schon immer wichtig, insbesondere in stark regulierten Branchen und im öffentlichen Sektor. In vielen Vertriebsgesprächen spielte sie jedoch eher eine Nebenrolle. Das ändert sich gerade.

Eine Gartner-Umfrage unter CIOs und IT-Verantwortlichen in Westeuropa vom November 2025 zeigte, dass **nur 2 Prozent** der Befragten davon ausgingen, dass geopolitische Entwicklungen ihre künftige Nutzung lokaler und regionaler Cloud-Anbieter nicht erhöhen werden, und **nur 8 Prozent** der Ansicht waren, dass geopolitische Fragen ihre künftige Nutzung globaler Cloud-Anbieter nicht einschränken werden.¹ In ganz Europa rückt Souveränität damit deutlich stärker in den Mittelpunkt von Kundengesprächen.

Souveränität ist heute nicht mehr nur ein Haken auf der Compliance-Checkliste. Sie ist zu einem wichtigen Nachweis dafür geworden, dass ein Anbieter das spezifische Umfeld und die Anforderungen seiner Kunden versteht. Es geht darum, den Markt zu kennen, in dem man aktiv ist – mit all seinen Besonderheiten. Die Frage lautet nicht mehr nur: „Können wir die DSGVO einhalten?“ Sondern vielmehr: **„Verstehen Sie diesen Markt, sind Sie ihm langfristig verpflichtet und können Sie hier zuverlässig liefern?“**

Das erhöht die Anforderungen an Service Provider, Technologieanbieter, Partner und das gesamte Ökosystem. Kunden stellen breitere und deutlich präzisere Fragen. Sie möchten nicht nur wissen, wo ihre Daten gespeichert werden, sondern auch, wie sie verarbeitet werden, wer darauf zugreifen kann, welche Gesetze möglicherweise Anwendung finden, welche Drittanbieter in der technischen Umgebung eingebunden sind und ob der Anbieter das lokale Betriebsumfeld wirklich versteht, in dem die Lösung eingesetzt wird.

Das ist eine deutlich größere Diskussion als: **„Liegen die Daten in Europa?“**

SOUVERÄNITÄT IST MEHR ALS DER SPEICHERORT VON DATEN

Eine der wichtigsten Veränderungen im Markt ist, dass Souveränität nicht mehr allein über den Speicherort der Daten definiert wird. Der Speicherort bleibt selbstverständlich wichtig, ist aber nur noch ein Teil eines deutlich größeren Fragenkomplexes.

Europäische IDC-Studien zeigen, dass der Schutz vor extraterritorialen Datenzugriffsanfragen heute der wichtigste Treiber für souveräne Cloud-Lösungen in Europa ist. Das ist jedoch nur ein Aspekt eines umfassenderen Souveränitätsverständnisses, das von geopolitischen Risiken, rechtlicher Exponierung, Abhängigkeiten und Autonomie geprägt ist.²

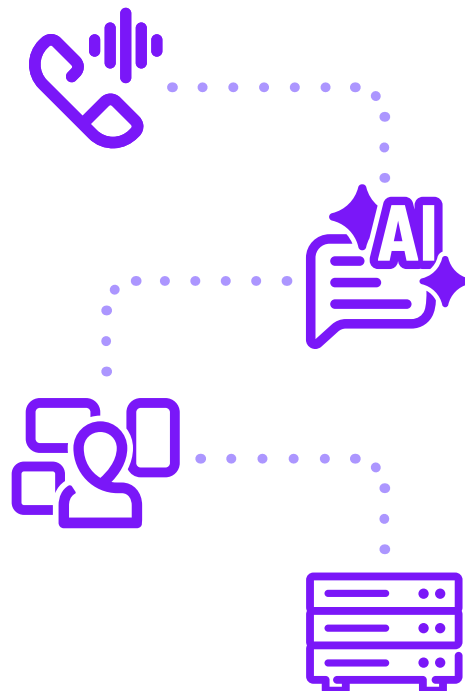
Kunden erwarten, dass Anbieter diese Diskussion souverän führen können. Sie sind sich der Herausforderungen rund um Daten-nutzung, Zugriffskontrollen, Unterauftragsverarbeiter, gesetzliche Risiken, Unternehmensstruktur und Dritttechnologien innerhalb einer Lösung immer stärker bewusst.

Vage Zusicherungen reichen nicht mehr aus. Ebenso wenig akzeptieren Kunden Anbieter und Reseller, die dem Thema sichtbar ausweichen, weil es unangenehm oder komplex wirkt. Sie erwarten die Sicherheit, dass der Anbieter und seine Partner die Thematik verstehen, sie anhand der konkreten Kundensituation erklären können und eine Lösung bieten, die auf den jeweiligen Markt und seine Realität zugeschnitten ist.

In der Praxis umfasst Souveränität heute operative Kontrolle, Herkunft und Eigentümerstruktur des Anbieters, Prozess-Compliance, gesetzliche Compliance und Nachvollziehbarkeit über die gesamte Servicekette hinweg. Gerade in unserer Branche ist das besonders relevant, weil Daten über mehrere Systeme hinweg fließen. Sprachaufzeichnungen können in ein CRM-System übernommen werden.

KI-Dienste können hinter Transkription, Zusammenfassung, Routing oder Automatisierungsprozessen stehen. Middleware, APIs und Workflow-Tools können Daten zwischen mehreren Anbietern übertragen. Auf dem Papier mag jedes Element beherrschbar wirken. In der Praxis ist die gesamte Kette oft deutlich schwieriger nachzuvollziehen, als viele Unternehmen annehmen.

Deshalb kann Souveränität nicht mehr als reine Pflichtübung behandelt werden. Es geht darum, ob ein Anbieter echtes Verständnis, Sicherheit im Umgang mit Komplexität und Glaubwürdigkeit im konkreten Kundenumfeld nachweisen kann.



„Es geht nicht nur darum, wo Daten liegen, sondern wer Zugriff hat – und wer die Kontrolle behält.“



EUROPA IST KEIN EINHEITLICHER MARKT

Wichtig bei der Betrachtung ist auch, dass Europa nicht zu stark vereinfacht wird.

Es gibt EU-weite Regelungen. Es gibt länderspezifische Gesetze. Es gibt EU-Richtlinien, die in den einzelnen nationalen Märkten unterschiedlich interpretiert und angewendet werden. Hinzu kommen branchenspezifische Erwartungen, vertragliche Anforderungen, lokale Gepflogenheiten und in manchen Ländern auch starke Mitbestimmungs- und Arbeitsrechtsstrukturen, die auf Unternehmensebene sehr spezifische operative Anforderungen schaffen können. All das beeinflusst, wie eine Lösung in der Realität implementiert und betrieben werden muss.

Kunden suchen keinen Anbieter, der lediglich aktuelle Anforderungen erfüllt. Sie suchen einen Anbieter, der versteht, wie sich diese Anforderungen entwickeln, Erfahrungen aus anderen europäischen Märkten einbringen kann und ihnen hilft, dem Markt voraus zu bleiben.

Ein Anbieter kann aus Sicht der Datensouveränität auf dem Papier stark wirken und in der Praxis dennoch scheitern, wenn er länderspezifische Anforderungen, lokale Geschäftspraktiken, sprachliche Erwartungen oder kulturelle Realitäten nicht versteht. Souveränität betrifft nicht nur den Ort, an dem eine Plattform gehostet wird. Es geht auch darum, ob ein Anbieter so arbeiten kann, dass er zu lokalen Erwartungen und Einschränkungen passt.

Ein Partner, der diese Realitäten nicht versteht, kann erleben, dass eine scheinbar regelkonforme Lösung an den tatsächlichen Anforderungen des Kunden vorbeigeht. Der europäische Markt muss deutlich differenzierter betrachtet werden.

„Europäische Souveränität“ ist kein einheitliches Anforderungspaket. Sie ist eine vielschichtige Kombination aus EU-, Länder- und Branchenanforderungen.

Die Verantwortung liegt beim Anbieter, den Kunden entsprechend zu beraten und durch das Thema zu führen.

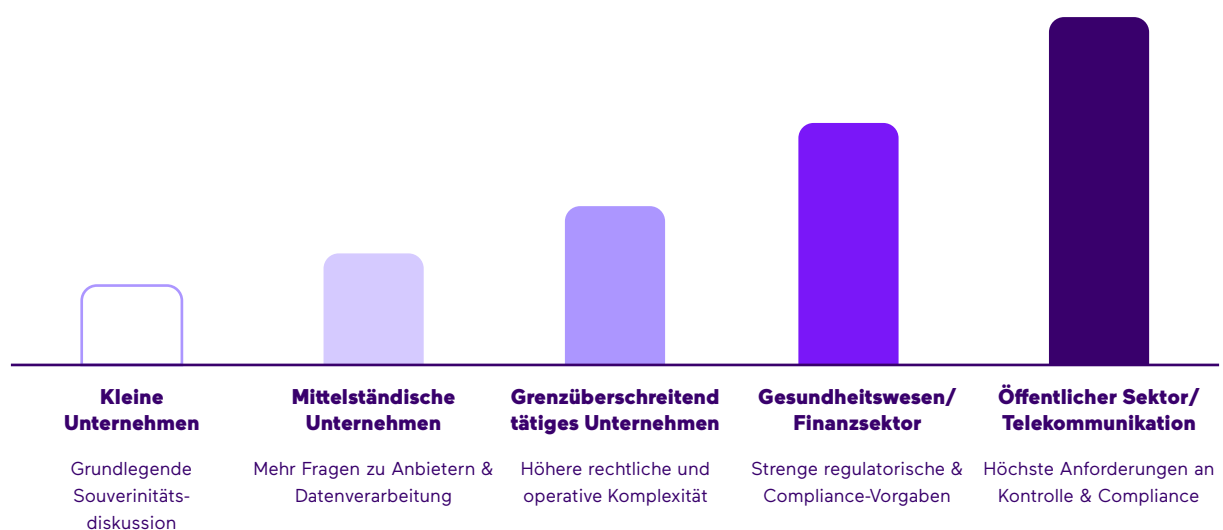
MANCHE KUNDEN LEGEN MEHR WERT AUF SOUVERÄNITÄT ALS ANDERE

Größere Organisationen stellen in der Regel detailliertere Fragen. Organisationen mit Nähe zum Staat, etwa Kommunen oder öffentliche bzw. staatsnahe Einrichtungen, sind häufig deutlich anspruchsvoller. Gesundheitswesen und Finanzdienstleister bleiben besonders sensibel. Auch Telekommunikationsanbieter betrachten nicht nur, wo Daten gespeichert werden, sondern auch die Herkunft von Infrastruktur und Software, das Bereitstellungsmodell und das gesamte Kontrollumfeld. Kunden, die grenzüberschreitend tätig sind, müssen zudem häufig ein komplexes Zusammenspiel nationaler Regulierungen entschlüsseln.

Für Partner bedeutet das: Der Vertriebsansatz muss entsprechend angepasst werden. Ein mittelständisches Unternehmen in einem weniger datenintensiven Umfeld kann mit einem deutlich schlankeren Gespräch

zufrieden sein, bei dem es stärker um Marktverständnis und Geschäftsmodell geht als um die exakte Bewegung jedes einzelnen Datenpunkts. Ein großer, regulierter oder staatsnaher Kunde kann dagegen mit einer langen Liste nicht verhandelbarer Anforderungen kommen. Beide Verkaufsprozesse gleich zu behandeln, wäre ein Fehler.

Gleichzeitig kann Souveränität auch bei kleineren oder weniger offensichtlich regulierten Kunden wichtiger sein, als es auf den ersten Blick scheint – insbesondere dann, wenn diese Unternehmen Teil einer größeren Lieferkette sind oder einen einfacheren Zugang zu sensibleren Systemen und Daten bieten. Jedes Unternehmen, das elektronische Zahlungen akzeptiert oder Daten über ein Netzwerk überträgt, kann unter bestimmte Anforderungen zur Datensouveränität fallen, unabhängig von seiner Größe.



DIE BEWEGUNG BESCHLEUNIGT SICH

Cybersecurity-Risiken, branchenspezifische Regulierung, geopolitische Spannungen und eine wachsende persönliche Verantwortung von Führungskräften verleihen der Souveränitätsdiskussion zusätzlichen Schub. Rahmenwerke wie DORA und NIS2 sind Teil dieser breiteren Entwicklung. Sie verstärken die Erwartung, dass Organisationen ihre Technologieumgebung genau verstehen, Risiken aktiv managen und Kontrolle nachweisen können. Die persönliche Verantwortung von Führungskräften erhöht die Dringlichkeit zusätzlich.

Dabei handelt es sich nicht nur um eine kommerzielle Entwicklung. Auch die EU selbst unterstützt das Thema mit erheblichen Investitionen und politischem Nachdruck. Im Oktober 2025 veröffentlichte die Europäische Kommission eine Ausschreibung über 180 Millionen Euro für souveräne Cloud-Lösungen³, die nur sechs Monate später an vier europäische Anbieter vergeben wurde. Hinter Souveränität steht also nicht nur Budget, sondern auch klarer Umsetzungswille. Auch einzelne Staaten investieren entsprechend. Allein die Schweizer Regierung investiert mehr als 350 Millionen Euro, um sicherzustellen, dass ihre staatlichen Cloud-Lösungen Anforderungen an Datensouveränität erfüllen.⁴

In einigen Märkten fühlen sich viele kleinere Unternehmen noch wohl mit der Aussage, dass ihre sensibelsten Daten, etwa E-Mails, ohnehin bereits bei großen internationalen Anbietern liegen. Für sie wirkt das wie eine unvermeidbare Realität moderner IT. Dieses Risikobewusstsein kann sich jedoch schnell verändern, wenn Abhängigkeit zunehmend wie Exponierung wirkt.

IDC-Studien vom Februar 2026 zeigen dies deutlich: 63 Prozent der Organisationen nutzen heute eher souveräne Cloud-Dienste, ausdrücklich aufgrund jüngster geopolitischer Ereignisse.⁵ Eine PwC-Studie vom November 2025 ergab, dass 82 Prozent der Organisationen ihren Cloud-Ansatz als Reaktion auf geopolitische und/oder regulatorische Veränderungen überarbeiten.⁶

Kleinere und weniger datensensitive Organisationen werden diesen Wandel wahrscheinlich nicht anführen. Sie werden jedoch tendenziell dem Weg folgen, den größere, stärker regulierte und souveränitätsbewusstere Käufer vorgeben. Die Richtung ist klar.

Für Partner ist das besonders relevant, weil sie keine kurzfristigen Entscheidungen für einzelne Verträge treffen. Sie investieren in Beziehungen zu Anbietern, die sie über Jahre hinweg im Markt vertreten möchten.

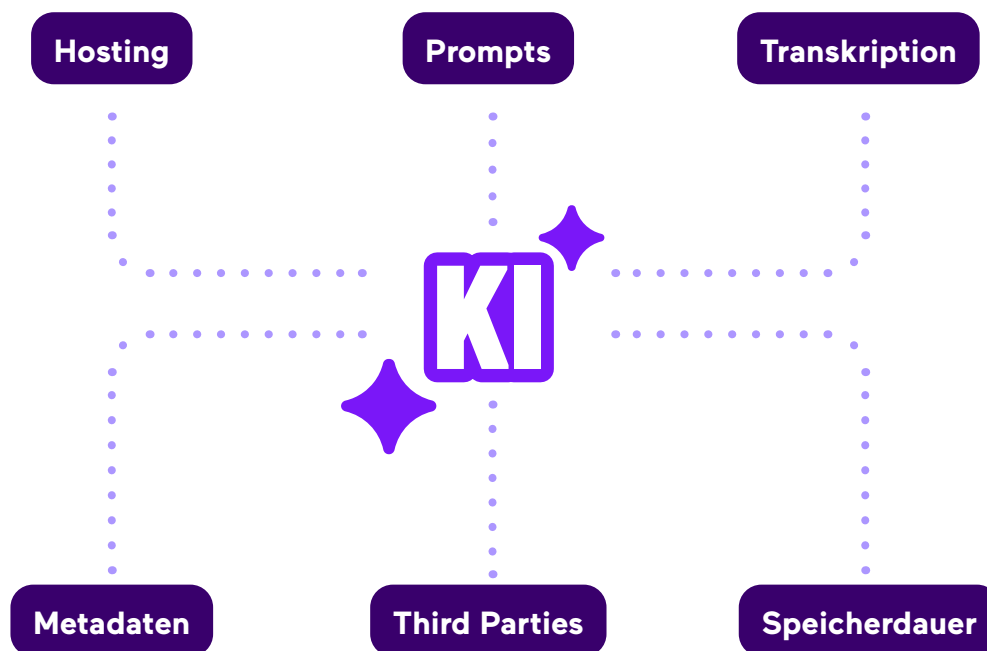
KI MACHT DAS THEMA NOCH DRINGLICHER

Souveränität hatte bereits an Bedeutung gewonnen, doch KI hat diese Entwicklung weiter beschleunigt.

Abgesehen von Cybersecurity-Aspekten werfen Voice AI, Transkription, Zusammenfassungen, Copiloten, LLM-basierte Automatisierung und intelligentes Routing neue Fragen auf: Welches Modell wird genutzt? Wo wird es gehostet? Handelt es sich um Multi-Tenant-SaaS oder um eine selbst gehostete Lösung? Welche Daten werden gespeichert? Welche Metadaten entstehen? Welche Drittanbieter sind beteiligt? Können Prompts, Ergebnisse, Aufzeichnungen oder Transkripte unerwartet Landesgrenzen überschreiten?

Je mehr intelligente Ebenen ein Anbieter in einen Dienst integriert, desto wichtiger wird es, klar zu erklären, wie dieser Dienst funktioniert und wie der Datenpfad aussieht. Eine Lösung kann aus Nutzersicht elegant erscheinen und darunter erhebliche Komplexität verbergen. Partner müssen disziplinierter darin werden, Souveränitätsanforderungen zu qualifizieren, weil Kunden erwarten, dass diese Sorgfalt bereits in ihrem Namen geleistet wurde.

Innovation ist für Kunden weiterhin attraktiv. Sie wird aber nur noch akzeptiert, wenn der Kunde das Betriebsmodell dahinter verstehen, steuern und ihm vertrauen kann.



NACHVOLLZIEHBARKEIT IST DER AUSGANGSPUNKT

Viele Unternehmen tun sich weiterhin schwer damit, Ende zu Ende nachzuvollziehen, wohin Daten fließen, welche Anbieter sie berühren, welche Dienste sie verarbeiten und welche Rechtsräume auf dem Weg relevant sein können.

Nachvollziehbarkeit gibt Partnern einen konkreten Ansatzpunkt. Sie macht Souveränität aus einem abstrakten Thema zu einem strukturierten Discovery-Prozess: Wo entstehen die Daten? Wo werden sie gespeichert? Wo werden sie verarbeitet? Welche Drittanbieter sind beteiligt? Welche Systeme tauschen Daten miteinander aus? Wer hat administrativen Zugriff? Wer hält die Verschlüsselungsschlüssel? Welche nationalen oder branchenspezifischen Anforderungen und Vorschriften gelten heute, und welche könnten während der Laufzeit der Lösung relevant werden?

Das sind wertvolle Vertriebsfragen, nicht nur Compliance-Fragen. Ein Partner, der Kunden durch diese Fragen führen kann, schafft früh im Prozess echten Mehrwert und vermeidet mit höherer Wahrscheinlichkeit schmerzhaftes Überraschungen zu einem späteren Zeitpunkt.

DER MARKT WIRD BREITER, NICHT KLEINER

Eine Multi-Tenant-Cloud bietet weiterhin große Vorteile bei Skalierbarkeit, einfacher Betriebsführung und Innovationsgeschwindigkeit. Für viele Kunden bleibt sie die richtige Lösung, insbesondere wenn sie lokal und regelkonform gehostet wird.

Gleichzeitig ist die Bandbreite sinnvoller Optionen größer. Private Cloud, hybride Bereitstellungen, landesspezifisch betriebene Instanzen und andere kontrollierte Bereitstellungsmodelle gewinnen wieder an Bedeutung, weil Kundenanforderungen noch vielfältiger werden. Die Diskussion dreht sich nicht um das Modell an sich, sondern darum, was es für den Kunden in Bezug auf Kontrolle, Compliance, Resilienz, Sicherheit und künftige Flexibilität bedeutet.

Käufer interessieren sich nicht abstrakt für ein Bereitstellungsmodell. Sie interessieren sich für Ergebnisse. Zunehmend geht es dabei nicht nur um Rechenzentren im eigenen Land, sondern auch um geografisch nahe Rechenzentren mit Backups im jeweiligen Land.

WAS BEDEUTET DAS FÜR PARTNER & SERVICE PROVIDER?

Die Chancen und Risiken sind klar. Souveränität ist ein kritischer Bestandteil des Kaufprozesses. Kunden brauchen Unterstützung, um die Komplexität zu verstehen und einzuordnen.

Die Gewinner werden diejenigen sein, die drei Dinge gut kombinieren: tiefes europäisches Verständnis auf Länderebene, praktische Nachvollziehbarkeit und flexible Bereitstellungsoptionen.

Genau hier werden zu 100 Prozent europäische, in Europa beheimatete und europäisch geführte Anbieter wie Enreach relevant. Käufer erwarten zunehmend mehr als eine Präsenz im jeweiligen Land, klare Architektur und flexible Bereitstellungsmodelle. Sie wünschen sich auch einen Anbieter mit fundiertem lokalen Wissen und breiter europäischer Erfahrung, der Erkenntnisse aus einem Markt nutzen kann, um Kunden und Partnern in einem anderen Markt einen Schritt voraus zu sein. Anbieter, die nicht nur technisch kompetent sind, sondern auch die Märkte verstehen, sind besser in der Lage, Partner und Endkunden durch die Komplexität von Souveränität zu führen.

Der Mehrwert für Partner ist enorm und wächst schnell. Gartner prognostiziert, dass die Ausgaben für souveräne Cloud-IaaS allein

in Europa von 6,9 Milliarden US-Dollar im Jahr 2025 auf 12,6 Milliarden US-Dollar im Jahr 2026 und 23,1 Milliarden US-Dollar im Jahr 2027 steigen werden.⁷

Kunden suchen zunehmend Anbieter, die sowohl auf europäischer als auch auf nationaler Ebene handlungsfähig sind. Sie wollen Anbieter, die das größere regulatorische Umfeld verstehen, aber auch wissen, dass lokale Marktgegebenheiten weiterhin entscheidend sind. Sie wollen Partner, die erklären können, wie Dienste funktionieren – nicht nur, wo ein Logo auf einer Karte steht. Und sie wollen Lösungen, die sich an echte Anforderungen anpassen lassen, statt jeden Kunden in dasselbe Modell zu pressen.

Souveränität ist kein Nischenthema, das in den Markt zurückkehrt. Sie wird Teil einer grundlegenden Neubewertung dessen, wie Vertrauen in Enterprise Communications und Customer Engagement beurteilt wird. Partner müssen Souveränität als strategisches Vertriebs- und Designthema behandeln, nicht als Compliance-Frage am Ende des Prozesses. Je klarer Sie Kundenanforderungen, Datenflüsse, Kontrollpunkte und lokale Verpflichtungen abbilden können, desto wertvoller werden Sie.

Und in einem Markt, in dem Vertrauen stärker geprüft wird als je zuvor, ist das eine starke Position.

Quellen:

- 1 [Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers](#)
- 2 [IDC's Digital Sovereignty In Europe 2025 Research](#)
- 3 [The European Commission moves forward on cloud sovereignty with a EUR 180 million tender](#)
- 4 [Swiss Government Cloud Project](#)
- 5 [IDC's cost of sovereignty research](#)
- 6 [PWC's November 2025 research on data sovereignty](#)
- 7 [Gartner's Feb 2026 research on sovereign cloud IaaS spending](#)

KONTAKTIEREN SIE UNS FÜR WEITERE INFORMATIONEN

Wenn Sie mehr über Cloud-Kommunikation und KI-Lösungen aus Europa für Europa erfahren möchten, nehmen Sie Kontakt zu uns auf. Wir beantworten gerne Ihre Fragen und stellen den Kontakt zu unseren lokalen Teams in ganz Europa her.

Kontaktieren Sie uns unter
info@enreach.com