2026 Daten-und Compliance Risiko: Datensouveränität in Europa

Der am stärksten regulierte Markt der Welt lernt weiterhin: Verträge können Gesetze nicht aushebeln – und die Architektur ist die wahre Verteidigung

Europa verfügt über das weltweit ausgereifteste Ökosystem für Datensouveränität. **Die DSGVO hat den globalen Standard gesetzt. NIS 2 und DORA verschärfen die Anforderungen an die operationelle Resilienz. Der Data Act gilt seit September 2025, die GPAI-Pflichten des EU AI Act traten im August 2025 in Kraft.** Europäische Unternehmen berichten von der höchsten kombinierten Kenntnis aller befragten Regionen – 80 % schätzen sich als „gut“ oder „sehr gut“ über Souveränitätsanforderungen informiert ein.

Doch die Reife hat das Risiko nicht beseitigt. Jeder dritte europäische Befragte hat in den letzten 12 Monaten einen Vorfall mit Bezug zur Souveränität erlebt. Das Vertrauensproblem gegenüber Anbietern bleibt bestehen: 44 % nennen Bedenken hinsichtlich der Souveränitätsgarantien von Anbietern als Hürde für die Nutzung europäischer Cloud-Lösungen. Und geopolitische Veränderungen – insbesondere US-Politikwechsel – verleihen Fragen neue Dringlichkeit, die das Schrems-II-Urteil eigentlich längst geklärt haben sollte. Diese Zusammenfassung fasst die wichtigsten europäischen Erkenntnisse aus einer regionsübergreifenden Umfrage in Kanada, dem Nahen Osten und Europa zusammen.

44%

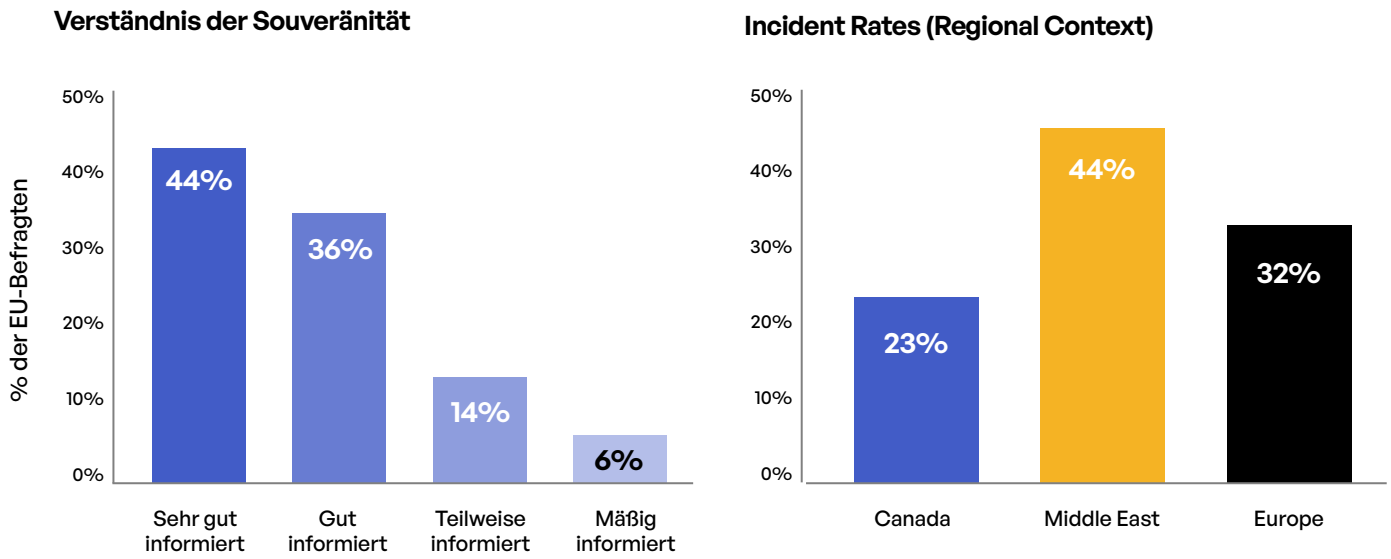
der europäischen Befragten nennen Bedenken hinsichtlich der Souveränitätsgarantien von Anbietern als Hürde – der höchste Wert aller Regionen und eine direkte Herausforderung für die Annahme „einfach EU-Rechenzentren nutzen“.

Regulatorische Reife hat die Vorfallslücke nicht geschlossen

Das Verständnis für Souveränität ist in Europa stark und breit verankert. 44 % fühlen sich „sehr gut informiert“, 36 % „gut informiert“, nur 6 % ordnen sich der niedrigsten Stufe zu. **Die DSGVO-Compliance ist nahezu universell. Die Bereitschaft für NIS 2 und DORA ist weit fortgeschritten, die meisten Unternehmen befinden sich in der „Implementierungsphase“ oder sind „weitgehend konform“.**

Dennoch haben 32,3 % der europäischen Befragten im vergangenen Jahr einen Souveränitätsvorfall erlebt – mehr als in Kanada (23,3 %), aber weniger als im Nahen Osten (44,4 %). Die häufigsten Vorfallarten sind unautorisierte grenzüberschreitende Übertragungen, regulatorische Untersuchungen, Datenschutzverstöße mit Souveränitätsbezug und Compliance-Fehler von Drittparteien. Die Botschaft ist klar: Regulatorische Reife reduziert, aber eliminiert Vorfälle nicht. Die verbleibende Lücke ist operativ, nicht informativ – und zu ihrer Schließung braucht es Architektur, nicht mehr Awareness-Trainings.

Die regulatorische Reife Europas hat Vorfälle nicht beseitigt — jeder Dritte meldet weiterhin einen



Souveränitätsverständnis unter europäischen Befragten (links) und Vorfallraten im regionalen Vergleich (rechts)

Der Business Case: Souveränität als europäischer Wettbewerbsvorteil

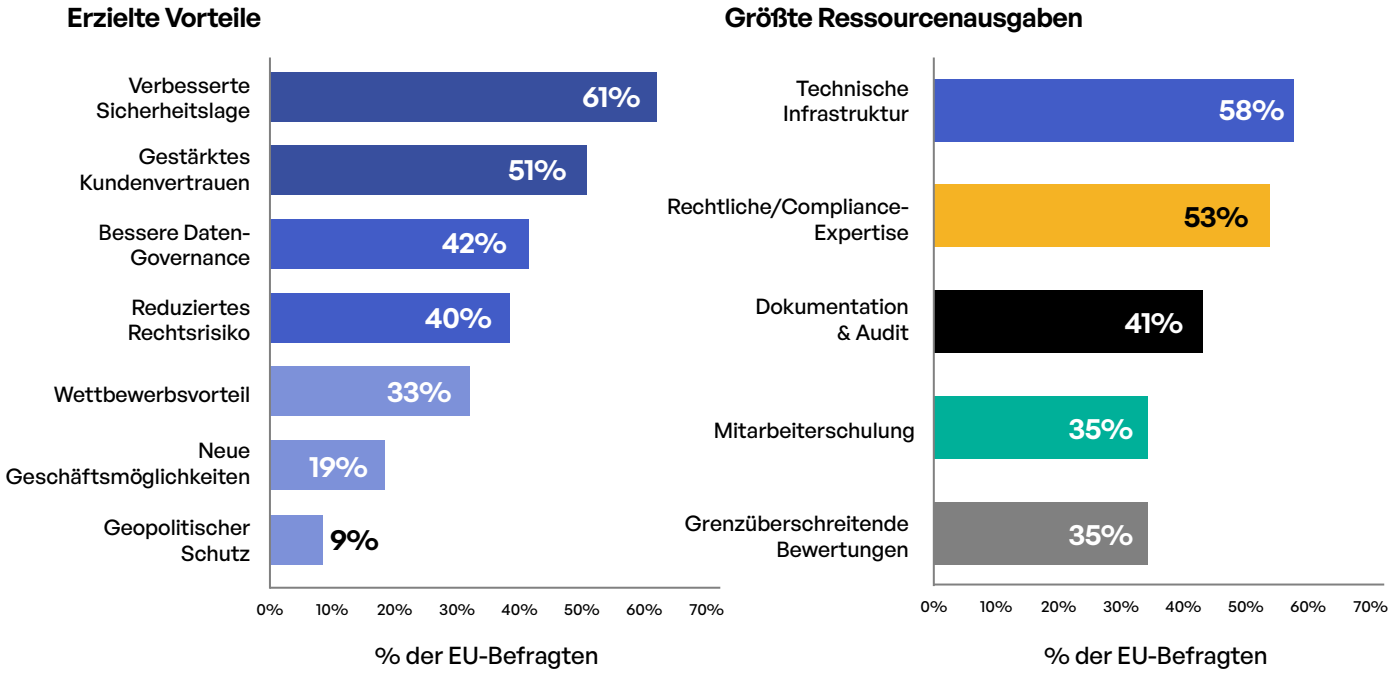
Europäische Befragte verbinden Souveränität mit konkretem geschäftlichem Mehrwert. **Verbesserte Sicherheitslage steht mit 61 % an erster Stelle, gefolgt von gestärktem Kundenvertrauen (51 %), besserer Daten-Governance (42 %), reduziertem Rechtsrisiko (40 %) und Wettbewerbsvorteil (33 %).** Diese Zahlen positionieren Souveränität nicht als regulatorische Last, sondern als Differenzierungsmerkmal im regulierungsbewussten europäischen Geschäftsumfeld.

Das Vertrauensdefizit gegenüber Anbietern ist Europas zentrale Souveränitätsherausforderung

44 % der Befragten äußern Bedenken, ob ihre Cloud-Anbieter tatsächlich Souveränität garantieren können. Eingeständnisse großer US-Anbieter zu Datenzugriffsbeschränkungen machen dies zu mehr als einer theoretischen Sorge. Das Schrems-II-Urteil hat klargestellt, dass Verträge ausländische Zugriffsrechte von Regierungen nicht aushebeln können. Die Konsequenz ist strukturell: Europäische Unternehmen können Souveränität nicht an die Zusagen eines Anbieters auslagern. Sie benötigen Kontrollen auf Architekturebene – Verwahrung der Verschlüsselungsschlüssel innerhalb der Jurisdiktion, Zugriffsrichtlinien auf Infrastrukturebene und Audit-Trails, die belegen, wo Daten gespeichert sind und wer darauf zugegriffen hat.

Der Ressourcenbedarf ist jedoch erheblich. Technische Infrastrukturänderungen führen mit 58 %, gefolgt von juristischer und Compliance-Expertise (53 %) sowie Dokumentation und Auditing (41 %). Beim Budget berichten 28 % der europäischen Befragten von jährlichen Souveränitätsbudgets über 5 Mio. €, weitere 31 % investieren 1–5 Mio. €. Bei Unternehmen mit mehr als 10.000 Beschäftigten fallen über 70 % in diese höchsten Ausgabenkategorien. Die Investitionen konzentrieren sich auf Bereiche, die nachweisbare Kontrolle schaffen: Durchsetzung des Datenstandorts, Verwahrung der Verschlüsselungsschlüssel, Automatisierung von Zugriffsrichtlinien und exportierbare Audit-Trails, die sowohl Regulatoren als auch Unternehmenskunden überzeugen.

Souveränität liefert klaren geschäftlichen Nutzen — bei erheblichen laufenden Kosten



Geschäftliche Vorteile durch Souveränitäts-Compliance (links) und wichtigste Ressourcenanforderungen (rechts)

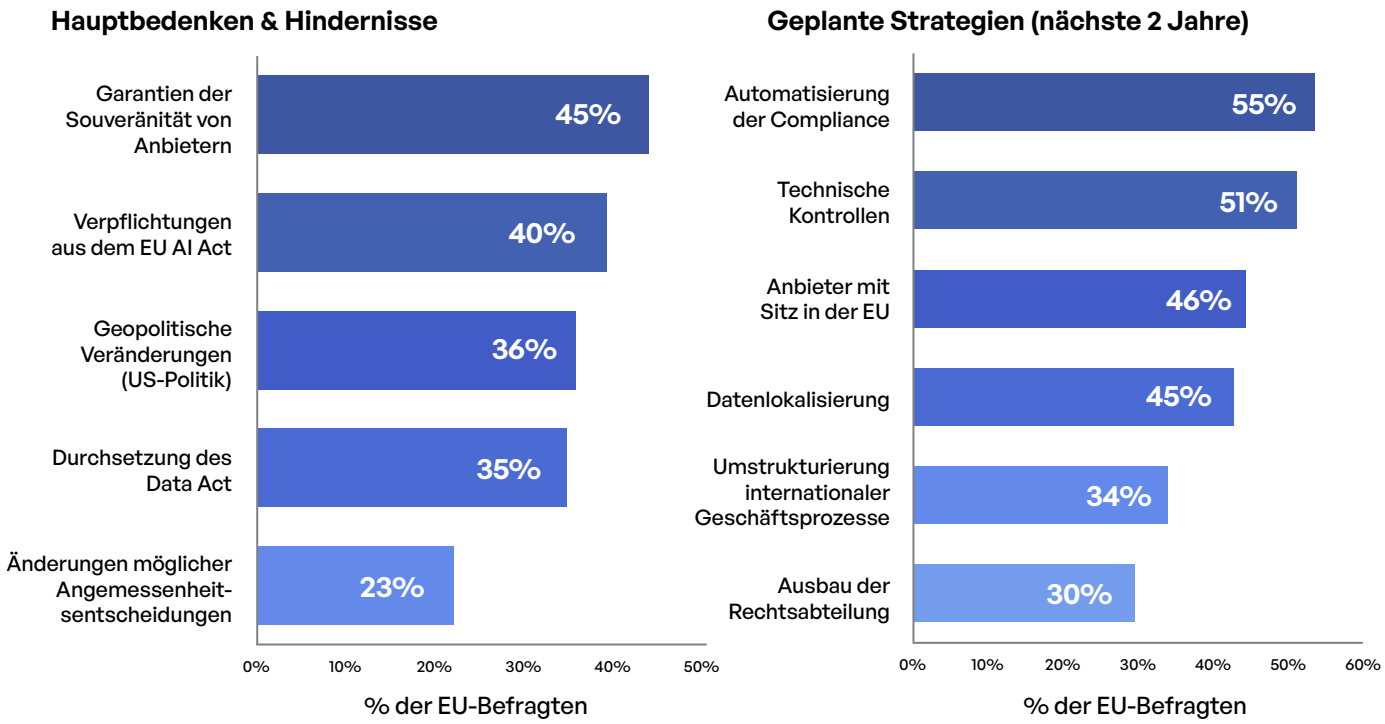
Die Kosten-Nutzen-Rechnung spricht für Unternehmen, die Souveränität als laufende betriebliche Disziplin und nicht als einmaliges Compliance-Projekt betrachten. Automatisierung ist der Effizienzhebel – 55 % planen in den nächsten zwei Jahren Investitionen in Compliance-Automatisierung, was sie zur wichtigsten Strategie in der Region macht.

Bedrohungslandschaft: Geschichtete Regulierung trifft auf Anbieterunsicherheit

Das Souveränitätsprofil Europas ist einzigartig komplex, weil es geschichtet ist. **Souveränitätsgarantien von Anbietern (44 %), der EU AI Act (40 %), US-Politikwechsel (36 %), Data-Act-Compliance (34 %) und mögliche Änderungen bei Angemessenheitsentscheidungen (23 %) erfordern gleichzeitig Aufmerksamkeit.** Keine andere Region steht vor so vielen parallelen regulatorischen Herausforderungen.

Die Planungsantwort spiegelt diese Komplexität wider. Compliance-Automatisierung liegt mit 55 % vorn, gefolgt von verbesserten technischen Kontrollen (51 %), Migration zu EU-basierten Anbietern (46 %), Datenlokalisierung (45 %), Restrukturierung internationaler Aktivitäten (34 %) und Ausbau der Rechtsabteilung (30 %). Europäische Unternehmen reagieren nicht auf eine einzelne Bedrohung – sie bauen geschichtete Verteidigungen, um geschichteter Regulierung zu begegnen. Erfolgreich sind diejenigen, die Souveränität in ihre Architektur integrieren, statt sie nur durch Richtlinien an bestehende Infrastruktur anzuflanschen.

Provider Trust Regulatory Layering Define Europe's Sovereignty Agenda



Wichtigste Bedenken und Hürden (links) und geplante Souveränitätsstrategien für die nächsten zwei Jahre (rechts)

AI-Governance: Vorbereitung auf den AI Act unter Souveränitätsauflagen

34 % der europäischen Befragten speichern sämtliche KI-Trainingsdaten innerhalb der EU, weitere 34 % nutzen einen gemischten Ansatz je nach Sensibilität der Daten. Die Einführung von Schutzmaßnahmen ist ausgeprägt: Regelmäßige KI-Audits stehen an erster Stelle, gefolgt von Impact Assessments für Hochrisiko-KI (48 %), Transparenzdokumentation, Einwilligungsmanagement und Bias-Tests.

Die GPAI-Pflichten des EU AI Act, die seit August 2025 gelten, haben das formalisiert, was viele Unternehmen bereits umsetzen. Doch die 34 %, die einen gemischten Ansatz verfolgen, müssen ihre Sensitivitätsklassifizierungen jetzt präzisieren – „je nach Sensibilität" ist kein belastbarer Standard, wenn die Kriterien nicht dokumentiert und revisionssicher sind. Unternehmen sollten sicherstellen, dass das KI-Daten-Governance in ihren übergreifenden Souveränitätsnachweis integriert ist – mit derselben auditfähigen Dokumentation wie für die DSGVO.

Souveränität, die Sie nachweisen können: Der europäische Standard

Europäische Aufsichtsbehörden verlangen zunehmend Belege statt Zusicherungen. Der Wandel geht von „wir glauben, konform zu sein" zu „wir können nachweisen, wo Daten liegen, wie Zugriffe gesteuert werden und wie grenzüberschreitende Übertragungen verhindert oder dokumentiert werden". Dafür braucht es drei Dinge. Kontrollen: Standortdurchsetzung, Verwahrung der Verschlüsselungsschlüssel und Zugriffsrichtlinien, die unautorisierte grenzüberschreitende Übertragungen auf Architekturebene verhindern. Nachweis-Artefakte: exportierbare Audit-Trails, Protokolle zum Datenstandort und Compliance-Reporting, das Regulatoren und Kunden auf Abruf überzeugt. Reaktionsbereitschaft: erprobte Playbooks für behördliche Datenzugriffsanfragen, Ausfälle von Drittanbietern, Transfer Impact Assessments und Schrems-II-Compliance-Szenarien. Unternehmen, die alle drei operationalisieren, machen regulatorische Komplexität zu einer verteidigungsfähigen Wettbewerbssituation.

Fünf Prioritäten für 2026

1. Schließen Sie die Vertrauenslücke zu Anbietern durch Architektur, nicht durch Verträge

44% nennen Bedenken zu Anbieter-Garantien. Die Antwort sind nicht bessere Zusicherungen, sondern Verwahrung der Verschlüsselungsschlüssel innerhalb der Jurisdiktion, Zugriffssteuerung auf Infrastrukturebene und nachweisbarer Datenstandort. Verträge können Gesetze nicht aushebeln – Architektur kann sie durchsetzen.

2. Investieren Sie in Compliance-Automatisierung, um regulatorische Schichtung zu bewältigen

55% planen dies bereits. Mit Data Act und AI Act, die nun neben NIS 2 und DORA gelten, ist manuelle Compliance nicht mehr tragbar. Automatisierung reduziert die technische Last (58 %) und liefert die revisionssicheren Nachweise, die Regulatoren verlangen.

3. Bereiten Sie sich jetzt auf die GPAI-Pflichten des AI Act vor

40% nennen den AI Act als Top-Thema. Unternehmen, die KI-Trainingsdaten lokalisiert und regelmäßige Audits vor der Durchsetzung eingeführt haben, sind im Vorteil. Wer noch an seiner KI-Datenstrategie arbeitet, ist bereits im Rückstand.

4. Entwickeln und testen Sie Playbooks für Schrems II und behördliche Zugriffsanfragen

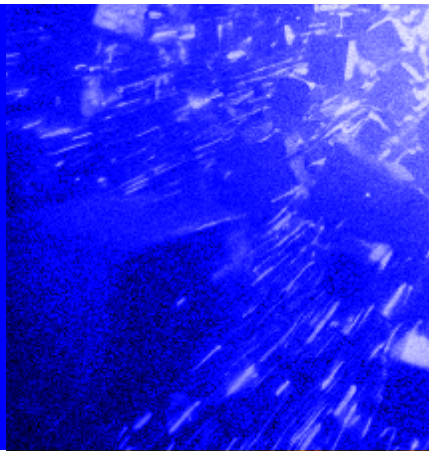
36% nennen geopolitische Veränderungen als Sorge. Transfer Impact Assessments müssen aktuell sein, DPF/SCC-Abhängigkeiten dokumentiert und die Reaktion auf grenzüberschreitende Übertragungen eingeübt – nicht nur geplant – werden.

5. Machen Sie Souveränität zu einem vertrauensbildenden Asset für Kunden

51% nennen gestärktes Vertrauen, 33 % Wettbewerbsvorteil. Im regulierungsbewussten europäischen Markt wird die Fähigkeit, Souveränität auf Abruf nachzuweisen – durch exportierbare Nachweise, nicht nur Richtliniendokumente – zur Voraussetzung für Unternehmensaufträge.

Kiteworks adressiert Datensouveränität

Dieser Bericht identifiziert das Vertrauensproblem gegenüber Anbietern als Europas zentrale Souveränitätsherausforderung – 44 % der Befragten äußern Bedenken, ob ihre Cloud-Anbieter tatsächlich Souveränität garantieren können, und das Schrems-II-Urteil bestätigt, dass Verträge ausländische Zugriffsrechte nicht aushebeln. Das Private Data Network von Kiteworks schließt diese Lücke. Die Bereitstellungsoptionen – On-Premises, Private Cloud, Hybrid und Single-Tenant-Hosting – ermöglichen es Unternehmen, sensible Inhalte ausschließlich innerhalb der EU-Infrastruktur zu speichern,



unabhängig von US-Anbietern, die dem CLOUD Act unterliegen. Kiteworks behält die Verwahrung der Verschlüsselungsschlüssel in der Jurisdiktion, setzt Geofencing durch konfigurierbare IP-Kontrollen um und wendet zero-trust-Architektur auf alle Kommunikationskanäle an: E-Mail, Filesharing, Managed File Transfer, SFTP und Datenformulare.

Für einen Markt, in dem Data Act, AI Act, NIS 2 und DORA nun gleichzeitig gelten, bietet Kiteworks zentrale Compliance-Kontrollen durch zentralisierte Audit-Logs, automatisiertes Reporting und vorkonfigurierte Templates für DSGVO, DORA, NIS 2 und PCI DSS. Die unveränderlichen Audit-Trails liefern die exportierbaren Nachweise, die diesen Wandel von „wir glauben, konform zu sein“ zu „wir können nachweisen, wo Daten liegen, wie Zugriffe gesteuert werden und wie grenzüberschreitende Übertragungen verhindert werden“ prägen. In Europas regulierungsüberlagerter Umgebung ist diese Nachweisfähigkeit der Schlüssel, um Souveränität von einer Compliance-Bürde in eine verteidigungsfähige Wettbewerbssituation zu verwandeln.

Für den vollständigen Bericht mit detaillierter Methodik, Branchenaufteilungen und regionaler Analyse, laden Sie ihn jetzt herunter.

Bericht herunterladen

Kiteworks