Kiteworks

LÖSUNGSBRIEF

FÜR CISOS, DATENSCHUTZBEAUFTRAGTE UND COMPLIANCE-VERANTWORTLICHE IN DEUTSCHLAND, ÖSTERREICH UND DER SCHWEIZ

Datensouveränität ist Architektur, keine Vertragsklausel

Ihre Daten. Ihre Rechtshoheit. Ihre Kontrolle.

Die Herausforderung im deutschen Markt

Deutschland verbindet einige der strengsten Datenschutzregeln der Welt mit der DSGVO und setzt sie über sechzehn eigenständige Landesdatenschutzbehörden neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) durch – eine Architektur muss also sechzehn regionalen Auslegungen genügen, nicht einem einzigen nationalen Standard. Das Bundesdatenschutzgesetz (BDSG) ergänzt Anforderungen, die die DSGVO allein nicht kennt: Ein Datenschutzbeauftragter ist bereits ab 20 Beschäftigten verpflichtend statt erst ab der allgemeinen DSGVO-Schwelle, § 26 BDSG regelt die Verarbeitung von Beschäftigtendaten im Detail, und vorsätzliche Verstöße können mit bis zu zwei Jahren Freiheitsstrafe geahndet werden – zusätzlich zu den Bußgeldern der DSGVO.

Dass Daten physisch in Deutschland liegen, beantwortet die eigentliche Frage nicht. Deutsche Kommentierungen zu den Datenresidenz-Anforderungen des EU AI Act bringen es unverblümt auf den Punkt: „Azure Germany oder eu-central-1 verschaffen Ihnen Datenresidenz, keine Datensouveränität – der US CLOUD Act reicht trotzdem hinein." Genau deshalb prüfen deutsche Aufsichtsbehörden internationale Datentransfers seit dem Schrems-II-Urteil besonders streng, und genau deshalb können vertragliche Zusagen eines Cloud-Anbieters eine Architektur nicht ersetzen, die das rechtliche Risiko von vornherein beseitigt.

Gleichzeitig wächst die Zahl der Anforderungen weiter. DSGVO und BDSG stehen inzwischen neben NIS-2, DORA (für deutsche Finanzinstitute durch die BaFin durchgesetzt), branchenspezifischen Regeln, die Gesundheits- und Telekommunikationsdaten zur lokalen Speicherung drängen, und einer wachsenden Welle öffentlicher Beschaffung, die Souveränität zunehmend als bindende Vertragsbedingung statt als Marketingaussage behandelt. Aufsichtsbehörden, Prüfer und mittlerweile auch Vergabestellen stellen dieselbe Frage: Können Sie mit Nachweisen – nicht mit Zusicherungen – belegen, wo Ihre Daten liegen, was ihren Abfluss verhindert und wer darauf zugegriffen hat?

Die Lösung

Kiteworks liefert Datensouveränität als Architektur, nicht als Vertragsklausel. Betrieb auf Single-Tenant-Infrastruktur – on-premises, in Ihrer eigenen Cloud oder als von Kiteworks gehostete Private Cloud – in Deutschland oder jedem Rechtsraum Ihrer Wahl, verschlüsselt mit Schlüsseln, die ausschließlich Sie besitzen.

Steuern Sie jeden Versand, jede Freigabe und jeden Download über die Geofencing-Regeln der Data Policy Engine, in Echtzeit durchgesetzt über jeden Kanal, den Menschen, Maschinen und Systeme zum Datenaustausch nutzen. Belegen Sie es mit einem vollständigen, ungedrosselten Audit-Trail, der live in Ihr SIEM einfließt – als Nachweis für den Bundesbeauftragten, jede der sechzehn Landesdatenschutzbehörden oder einen BaFin-Prüfer, je nachdem, wer fragt.

Warum Souveränität in Deutschland zur Vorstandsfrage geworden ist

- **44 %** der europäischen Organisationen bezweifeln, dass ihr Cloud-Anbieter Datensouveränität tatsächlich garantieren kann – der höchste Wert aller untersuchten Regionen und eine direkte Widerlegung der Annahme, ein europäisches Rechenzentrum allein genüge (Kiteworks Europe Sovereignty Report).
- **250 Millionen Euro** Wert des „Deutschland-Stack", des KI-Cloud-Vertrags der Bundesregierung, im Mai 2026 an zwei inländische Konsortien vergeben, ohne Beteiligung eines US-Hyperscalers und mit verbindlichen Bring-Your-Own-Key- und Zero-Trust-Anforderungen (Bundesministerium für Digitales und Staatsmodernisierung, laut Cloud Magazin).
- **16** eigenständige Landesdatenschutzbehörden setzen BDSG und DSGVO neben dem Bundesbeauftragten durch – Nachweise müssen also regionalen Unterschieden standhalten, nicht nur einer einzigen nationalen Auslegung (globaldatashield.com).

Wie Kiteworks nachweisbare Souveränität liefert

Single-Tenant von Grund auf

Dedizierte Infrastruktur ohne gemeinsame Datenbanken, Dateisysteme, Anwendungslaufzeiten oder Betriebssysteme. Betrieb on-premises, in Ihrer eigenen Cloud oder als von Kiteworks gehostete Single-Tenant-Private-Cloud, in Deutschland oder dem Rechtsraum Ihrer Wahl. Genau dieses Prinzip schreibt die Bundesregierung inzwischen selbst verbindlich in Vergabeunterlagen fest: Die Deutschland-Stack-Ausschreibung setzt fehlende gemeinsame Infrastruktur zwischen Mandanten als Zuschlagsvoraussetzung voraus – nicht als Marketingaussage.

Kundeneigene Verschlüsselungsschlüssel

Durch HSM-Integration kann weder Kiteworks noch eine Partei, die Kiteworks dazu zwingt, Ihre Daten entschlüsseln – auch nicht bei einer verdeckten behördlichen Anordnung. Es ist dieselbe Logik wie beim Bring-Your-Own-Key-Mandat des Deutschland-Stack und bei der öffentlichen Zusage der Deutschen Telekom zu ihrer Nvidia-gestützten KI-Cloud in München, dass „nur zertifizierte Mitarbeitende aus Deutschland und anderen europäischen Unternehmen" Zugriff erhalten.

Geofencing beim Datenabfluss

Die Data Policy Engine blockiert Versand und Freigaben oder verlangt eine Freigabe – und kann Downloads vollständig unterbinden – basierend auf Geolokation, gesperrten Ländern und IP-Bereichen. Das adressiert genau das, was deutsche Aufsichtsbehörden seit Schrems II prüfen: nicht, wo Daten liegen, sondern ob und wie sie das Unternehmen verlassen können.

Eine Control Plane für jeden Kanal

E-Mail, Filesharing, SFTP, MFT, APIs und KI-Agenten unterliegen alle denselben Egress-Richtlinien. Für Menschen, Maschinen und Systeme entstehen keine kanalspezifischen Lücken, durch die Daten entweichen könnten.

Vollständiger, ungedrosselter Audit-Trail

Jede Aktion von Nutzenden, Administratoren und Systemen wird in Echtzeit protokolliert und live an Ihr SIEM übergeben, ohne Stichprobenbildung und ohne Drosselung bei hoher Last – bereit als Nachweis für den Bundesbeauftragten, jede der sechzehn Landesdatenschutzbehörden oder eine BaFin-Prüfung, unabhängig davon, wer anfragt.

Geprüft nach anerkannten Standards

Die Architektur von Kiteworks ist nach ISO/IEC 27001 validiert, ergänzt um ISO/IEC 27017 für Cloud-Sicherheit und ISO/IEC 27018 für den Schutz personenbezogener Daten. DSGVO-Compliance-Reports, Bestandteil von Advanced Governance, unterstützen unmittelbar die sich überschneidenden Anforderungen des BDSG – Audit-Logs, die auf die §§ 22 Abs. 2, 62 Abs. 5, 64 Abs. 3 und 70 BDSG abgebildet sind und dokumentieren, wer personenbezogene Daten aufgerufen, verändert oder übertragen hat. Kiteworks hat zudem das strenge Prüfverfahren von FedRAMP durchlaufen (FedRAMP High In Process; FedRAMP Moderate Authorized seit 2017) – dieselbe Art unabhängiger, evidenzbasierter Prüfung, wie sie Deutschland mit dem C5-Kriterienkatalog des BSI und dem entstehenden C3A-Souveränitätskatalog inzwischen von Cloud-Anbietern der öffentlichen Hand verlangt.

Wo Souveränität in Deutschland nicht verhandelbar ist

Behörden und öffentlicher Sektor

Bürgerdaten unter einer Nationalen Rechenzentrumsstrategie, die Rechenzentren seit März 2026 formal als kritische Infrastruktur einstuft – und unter Vergabemandaten wie dem Deutschland-Stack, die Souveränität inzwischen als bindende Vertragsbedingung festschreiben.

Automobilindustrie und Fertigung

Die deutsche Automobil-Lieferkette basiert auf TISAX-Prüfungen (Trusted Information Security Assessment Exchange) zwischen OEMs und Zulieferern. Sicheres, zugriffsgesteuertes Filesharing und vollständige Audit-Nachweise unterstützen genau die Informationssicherheitskontrollen, die TISAX-Assessments prüfen.

Finanzdienstleistungen

Kunden-, Handels- und Risikodaten unter dem Prüfungsregime der BaFin für operationale Resilienz und Auslagerungen sowie unter den IKT-Risikoanforderungen der DORA, wie sie die BaFin national durchsetzt.

Gesundheitswesen und Life Sciences

Patientendaten unter den besonderen Schutzvorschriften des BDSG für sensible Datenkategorien, ergänzt um Vorgaben des Sozialgesetzbuchs und landesrechtliche Krankenhausgesetze, die eine lokale Speicherung vorschreiben können, sowie Forschungsdaten mit eigenen Residenzanforderungen.

Quellen

Kiteworks, „2026 Data Security and Compliance Risk: Data Sovereignty in Europe“ (Executive Summary), Februar 2026.
„250 Million Euros for the Federal AI Cloud“, Cloud Magazin, 19. Juni 2026.
„Data Residency in Germany: BDSG Compliance Guide“, globaldatashield.com.
„German Government Adopts National Data Center Strategy“, Morgan Lewis, April 2026.
„ITC Giants Pair to Build Massive Sovereign German Data Center“, gtai.de.
„EU AI Act Data Sovereignty: Frankfurt Region Isn’t Enough“, particula.tech.

www.kiteworks.com

Juli 2026