



KI-Souveränität

Sind KI-Daten ohne Souveränität wirklich sicher?

Sind KI-Daten ohne Souveränität wirklich sicher?

Im hochgradig dynamischen Umfeld der künstlichen Intelligenz müssen Unternehmen zunehmend darauf achten, dass ihre KI-Modelle und wertvollen Daten nur in bestimmten Regionen ausgeführt und verarbeitet werden. Diese sogenannte KI-Souveränität ist erforderlich, da moderne Systeme sensible Daten verarbeiten und proprietäre Modelle nutzen. Dadurch entstehen komplexe Herausforderungen in Bezug auf Verantwortlichkeit, Nachvollziehbarkeit und Daten-Governance¹.

“

Wenn Sie unternehmensinternes Wissen nicht in den Gewichtungen Ihres Modells festhalten können, fehlt Ihnen die nötige Souveränität. Ihr proprietäres Wissen kann nach außen gelangen und in andere Modelle integriert werden².“

Satya Nadella,
CEO von Microsoft

Das Konzept der Souveränität umfasst heute mehr als nur den Speicherort von Daten. Vielmehr stellt sich die Frage, wer den physischen Standort kontrolliert, an dem Rechenprozesse stattfinden.³ Unternehmen können ihre Autonomie und Datensicherheit wahren, ihre operative Resilienz stärken und wettbewerbsfähig bleiben, indem sie ihre KI-Systeme dezentralisieren, Abhängigkeiten von externen Anbietern beseitigen und Open-Source-Modelle nutzen.



¹. Stanford University, AI Sovereignty's Definitional Dilemma, <https://hai.stanford.edu/news/ai-sovereignty-s-definitional-dilemma>, 2026

². The Register, Speed: Microsoft CEO: AI sovereignty isn't where it runs, it's who controls it, <https://www.theregister.com/software/2026/01/21/nadella-talks-ai-sovereignty-at-the-world-economic-forum/5128191>, 2026

³. 3. Red Hat, What is Sovereign AI? <https://www.redhat.com/en/topics/ai/sovereign-ai>, 2026



KI-Verantwortliche benötigen eine mehrschichtige Kontrolle

Angeichts dieser komplexen Entwicklungen dürfen sich Führungskräfte nicht auf undifferenzierte und vereinfachende Vorstellungen von „Kontrolle“ verlassen. Sie benötigen durchdachte, mehrschichtige Strategien, die gezielt auf die verschiedenen Aspekte ihrer betrieblichen Prozesse abzielen⁴. So zeigt beispielsweise ein Bericht von Cisco, dass ein KI-Agent 450 % mehr Netzwerkverkehr erzeugt als ein Mensch, der dieselbe Aufgabe manuell ausführt⁵. Künftig könnte es daher notwendig werden, den Datenverkehr von Menschen und KI-Agenten über getrennte Infrastrukturen abzuwickeln und Komponenten wie Datenstandort, Modelleigentum und operative Governance gesondert zu berücksichtigen.

Für jede dieser Komponenten müssten dann maßgeschneiderte Ansätze angewendet werden.

Zu den wichtigsten Konzepten gehören:

- Territoriale Kontrolle: Kontrolle über die physischen Standorte von Daten- und Rechenressourcen.
- Operative Kontrolle: Verwaltung und Absicherung dieser kritischen Ressourcen.
- Technologische Kontrolle: Materielle und geistige Eigentumsrechte an der Infrastruktur und den Algorithmen.

“

Laut einer Prognose von IDC werden multinationale Unternehmen ihre Investitionen in souveräne, lokal betriebene Cloud- und Datenumgebungen mit modularem Aufbau bis 2028 um 65 % erhöhen. Damit sollen Prozesse zukunftsfähig gestaltet und die steigenden Anforderungen an die Datenhoheit erfüllt werden⁶.

⁴ Kyndryl, Lovejoy, The physical foundations of digital sovereignty: How to reclaim control in the age of AI, <https://www.kyndryl.com/gb/en/insights/articles/2026/04/ai-sovereignty-enterprise-control>, 2026

⁵ Cisco, AI Impact on Wide Area Networks, <https://www.cisco.com/c/dam/en/us/solutions/collateral/artificial-intelligence/mass-scale-infrastructure/ai-network-traffic-report.pdf>, 2026

⁶ IDC, Claps and Nasir, Dispelling the myth of a silver bullet in sovereign, <https://www.idc.com/resource-center/blog/dispelling-the-myth-of-a-silver-bullet-in-sovereign-ai/>, 2026



Vertrauenswürdige Daten verändern europäische Lieferketten

BMW vernetzt seine Lieferketten mithilfe von Catena-X. Das offene, kollaborative Datenökosystem ermöglicht den sicheren und standardisierten Austausch von Daten⁷.

BMW nutzt Catena-X als Instrument der Transparenz, beispielsweise zur Berechnung des CO₂-Fußabdrucks von Bauteilen und zur Stärkung der Krisensicherheit durch die frühzeitige Erkennung von Engpässen. Pilotprojekte zeigen, dass diese Initiative den Informationsfluss verbessert und somit zu mehr Nachhaltigkeit und Effizienz in der digitalen Lieferkette von BMW führt. Dadurch werden letztlich die Wertschöpfungsketten der gesamten Branche aufgewertet⁸.

Das Luftfahrtunternehmen Airbus entwickelt einen vertrauenswürdigen Datenraum für den sicheren Datenaustausch mit rund 10.000 Zulieferern⁸. Als Teil der EU-Initiative Gaia-X für souveräne Datenräume soll diese Plattform gewährleisten, dass sensible Betriebs- und Konstruktionsdaten unter europäischer Kontrolle bleiben. Dadurch werden unerwünschte Abhängigkeiten vermieden und das Vertrauen gestärkt.

Durch die Nutzung eines föderierten, souveränen Datenmodells stellt Airbus die Datenautonomie der beteiligten Partner sicher. Dieser Ansatz stärkt die Krisenresistenz, Sicherheit und Zusammenarbeit in der europäischen Luft- und Raumfahrtindustrie. Gleichzeitig werden Innovationen und digitale Souveränität gefördert.

⁷ BMW Group, On the way to a digitally connected supply chain with Catena-X, <https://www.bmwgroup.com/en/news/general/2025/catena-x-connects-digital-supply-chains.html>, 2025

⁸ Raconteur Magee, Why Airbus is all-in on EU data project Gaia-X, <https://www.raconteur.net/technology/why-airbus-is-all-in-on-eu-data-project-gaia-x>, 2024

Können Unternehmen ihre KI-Systeme überhaupt besitzen?



Die Umstellung von einem externen KI-Dienst der Premiumklasse auf ein eigenes Modell kann einen laufenden Kostenfaktor in einen wertvollen strategischen Vorteil verwandeln. Für große Unternehmen wird es zunehmend schwieriger, die hohen Ausgaben für KI zu rechtfertigen. Viele Führungskräfte mussten ihre anfänglich optimistischen Kostenprognosen korrigieren. So hat Uber beispielsweise sein gesamtes KI-Budget für 2026 bereits nach vier Monaten aufgebraucht⁹. Genau hier setzen Unternehmen wie Mistral an, die eine Demokratisierung der künstlichen Intelligenz durch quelloffene, effiziente und innovative Modelle, Produkte und Lösungen fördern¹⁰.

Hannah-Marie Darley, Mitbegründerin und CAIO von Geordie AI, erklärt: „KI-Souveränität ist mit hoher Wahrscheinlichkeit nur durch Partnerschaften mit anderen Unternehmen und Ländern erreichbar. Selbst wenn sich der Speicherort der Daten zuverlässig kontrollieren lässt, kann die Funktionalität kaum umfassend gewährleistet werden. Die aktuell führenden Modelle sind das Resultat von Investitionen in Milliardenhöhe. Eigenentwicklungen einzelner Unternehmen werden da nicht mithalten können¹¹.“

“

Ich kann absolut nachvollziehen, warum Unternehmen diesen Ansatz wählen. Schließlich haben sie bereits viel Geld in eigene KI-Modelle investiert und möchten diese nicht in die Cloud auslagern. In der Regel ist lokales Hosting auch wirtschaftlich sinnvoller. Zudem kann so sichergestellt werden, dass die Daten und Algorithmen optimal geschützt sind.“

Colin Wilson,
Enterprise Architect, Verizon Business

⁹. Fortune, Angelo, Uber burned through its entire 2026 AI budget in four months. Now its COO is questioning whether it's worth it, <https://fortune.com/2026/05/26/uber-coo-ai-spending-tokens-claude-code/>, 2026

¹⁰. Matt Turck, LinkedIn-Beitrag, abrufbar unter: https://www.linkedin.com/posts/turck_while-silicon-valley-obsesses-over-agi-mistral-ugcPost-7427752521298821120-BLOm/, 2026

¹¹. IT Brew, Monsanto, What is AI sovereignty and why are companies chasing after it? <https://www.itbrew.com/stories/2026/04/27/what-is-ai-sovereignty-and-why-are-companies-chasing-after-it>, 2026



KI-Souveränität meistern: Ein mehrschichtiger Ansatz

Der Besitz der zugrunde liegenden Infrastruktur macht KI zu einem strategischen Erfolgsfaktor. Um jedoch vollständige Souveränität zu erlangen, ist eine komplexe und vielschichtige Kontrolle erforderlich. Datensouveränität lässt sich nicht allein durch Vorschriften und Richtlinien gewährleisten. Die digitale Tokenisierung ermöglicht hingegen die Interoperabilität der vernetzten Systeme und einen kontinuierlichen Informationsfluss, während personenbezogene und regulierte Daten geschützt bleiben. Die tokenisierten Daten können frei über Analysesysteme, KI-Pipelines und Partnernetzwerke hinweg übertragen werden, ohne dass konkrete Inhalte preisgegeben werden¹².

Warum ist das wichtig?

Im KI-Umfeld müssen Unternehmen zunehmend auf den Schutz ihrer wertvollen Daten und Infrastrukturen achten. Ohne KI-Souveränität drohen komplexe Herausforderungen, Kostenspiralen und ein Mangel an Flexibilität:

- Verantwortlichkeit, Nachvollziehbarkeit und Governance von sensiblen Daten und proprietären Modellen sind gefährdet.
- Bei fehlender Kontrolle über Modelle mit integriertem internem Wissen kann proprietäres Wissen nach außen gelangen.

- Unternehmen lassen die Chance ungenutzt, KI mit ihren eigenen Daten zu trainieren und effizientere Möglichkeiten zur Nutzung und Wertschöpfung ihrer Daten zu schaffen.

Was bedeutet das?

Das Konzept der KI-Souveränität umfasst neben der Datenresidenz auch die Kontrolle über den Standort, an dem Rechenprozesse ausgeführt werden. Dadurch ergeben sich die folgenden Anforderungen:

- Dezentralisierung von KI-Ressourcen, Unabhängigkeit von externen Anbietern und sichere Datenverarbeitung in verteilten Umgebungen durch digitale Tokenisierung
- Gegebenenfalls der Aufbau eines vollständigen KI-Technologie-Stacks
- Eine mehrschichtige Kontrollstrategie unter Berücksichtigung territorialer (Standort), operativer (Verwaltung) und technologischer (eigene Infrastruktur, geistiges Eigentum) Überlegungen
- Nutzung von Open-Source-Modellen zur Stärkung der autonomen Datensicherheit, der operativen Resilienz und der Wettbewerbsfähigkeit

¹² ALTR, AI sovereignty demands more than borders—it requires control over how data behaves. Digital tokenization is the key to that control, <https://altr.com/blog/without-digital-tokenization-there-is-no-sovereign-ai/>, 2026

Die Folgen

Unter Berücksichtigung der folgenden Einschränkungen kann KI-Souveränität laufende Kosten in einen wertvollen strategischen Vorteil für das Unternehmen verwandeln:

- In Bereichen der nationalen Sicherheit und der kritischen Infrastruktur ist es mitunter erforderlich, vollständige Souveränität zu erlangen und mit den neuesten KI-Modellen Schritt zu halten. In anderen Anwendungsfällen ist die digitale Tokenisierung der richtige Ansatz, um sicher zusammenzuarbeiten und Informationen auszutauschen, ohne Rohdaten preiszugeben.
- Die eigenständige Entwicklung und Pflege komplexer Modelle kann sich als zu ambitioniert erweisen, zumal diese aufgrund der milliardenschweren Investitionen globaler Akteure möglicherweise nicht konkurrenzfähig sind.

Wissenswertes

Führungskräfte müssen durchdachte und vielschichtige KI-Strategien entwickeln, die über vereinfachende Ansätze hinausgehen.

- Bis 2028 werden multinationale Unternehmen ihre Investitionen in modulare, souveränitätsfähige Cloud-Umgebungen voraussichtlich um 65 % erhöhen. Die digitale Tokenisierung ist eine Schlüsseltechnologie, um die Datenströme in diesen Umgebungen abzusichern¹³.
- Obwohl Unternehmen wie Mistral mit Open-Source-Lösungen zur Demokratisierung der künstlichen Intelligenz beitragen, sind für umfassende Souveränität gemeinsame Initiativen erforderlich¹⁴.



¹³. IDC, Claps and Nasir, Dispelling the myth of a silver bullet in sovereign AI, <https://www.idc.com/resource-center/blog/dispelling-the-myth-of-a-silver-bullet-in-sovereign-ai/>, 2026

¹⁴. Raconteur Magee, Why Airbus is all-in on EU data project Gaia-X, <https://www.raconteur.net/technology/why-airbus-is-all-in-on-eu-data-project-gaia-x>, 2024

Welche Auswirkungen hat KI-Souveränität auf das Netzwerk?

Um vollständige KI-Souveränität zu erreichen, ist ein mehrschichtiger Ansatz erforderlich, der territoriale, operative und technologische Kontrollmechanismen umfasst. Die Umsetzung ist nicht nur ein strategisches Ziel, sondern auch eine praktische Notwendigkeit mit weitreichenden

betrieblichen und infrastrukturellen Auswirkungen. Die folgende Tabelle veranschaulicht, wie sich relevante Geschäftsziele in konkrete KI-Anforderungen umsetzen lassen und welche Leistungsparameter die Infrastruktur für eine umfassende KI-Kontrolle aufweisen muss.

Geschäftsziel	KI-Anforderung	Auswirkung auf das Netzwerk
Verantwortlichkeit, Nachvollziehbarkeit und Daten-Governance	Strenge Vorgaben für die Datenresidenz, die sicherstellen, dass sensible Daten und proprietäre Modelle nur in rechtlich geschützten Räumen verarbeitet bzw. betrieben werden.	Robuste Netzwerksegmentierung, geografische Zugriffskontrolle und verschlüsselte Verbindungen, um die Datenresidenz zu gewährleisten und die unbefugte Übertragung von Daten über Landesgrenzen hinweg zu verhindern.
Schutz von proprietärem Wissen und geistigem Eigentum	Sicheres Trainieren, Implementieren und Verwalten von KI-Modellen bei voller technologischer Kontrolle über Algorithmen, Gewichtungen und das integrierte interne Wissen.	Sichere, isolierte Netzwerke für die Entwicklung und produktive Nutzung von KI-Modellen mit strenger Kontrolle des ausgehenden Datenverkehrs und Angriffserkennung zum Schutz des geistigen Eigentums und der Modellintegrität.
Betriebliche Resilienz und Unabhängigkeit von externen Anbietern	Autonomie durch dezentrale KI-Modelle mit Edge-Computing und föderiertem Lernen an verschiedenen physischen Standorten sowie in souveränen Clouds.	Eine ausfallsichere, latenzarme, skalierbare und verteilte Architektur für unterschiedliche Workloads und lokale KI-Hardware mit konsistenter Leistung.
Sicherer und zuverlässiger Datenaustausch über Partnernetzwerke	Ein kontrollierter und nachvollziehbarer Austausch von Daten und Modellausgaben zwischen Partnern, wobei die Souveränität der Partner in der Regel durch Token zum Schutz sensibler Informationen gewährleistet wird.	Zuverlässiger Datenaustausch über sichere Verbindungen in einer Zero-Trust-Architektur (ZTA), ergänzt durch geschützte API-Gateways für kontrollierte Datenströme sowie präzise Zugriffsregeln zur Gewährleistung von Informationssicherheit und Compliance.
Mehrschichtige Compliance-Strategie	Durchsetzung separater Richtlinien für die territoriale (Standort), operative (Verwaltung) und technologische (eigene Infrastruktur, geistiges Eigentum) Kontrolle.	Flexible, softwaredefinierte Netzwerke für die schnelle Anwendung präziser Richtlinien, die Steuerung des Datenverkehrs und Unterstützung der Compliance-Anforderungen an allen IT-Standorten.
Umwandlung von KI von einem laufenden Kostenfaktor in einen strategischen Vorteil	Möglichkeiten für die interne Entwicklung, Bereitstellung und das Training von KI-Systemen, einschließlich der Integration von Open-Source-Modellen in ein souveränes Ökosystem.	Zuweisung leistungsfähiger interner Netzwerkressourcen für die Verarbeitung großer Datenmengen und das Modelltraining, um die Kosten für interne Datentransfers zu optimieren und die Effizienz der eigenen Infrastruktur für KI-Workloads zu steigern.

Unser Beitrag für eine souveräne KI

Zweifellos wird der Weg zur KI für Verizon und zahlreiche andere Unternehmen weltweit viele weitere Schritte umfassen.

Wir von Verizon konzentrieren uns dabei vorwiegend auf Transparenz, Erklärbarkeit und menschliche Aufsicht. Wir haben gelernt, wie wir das Vertrauen in KI-Systeme stärken und unsere Belegschaft auf KI-gestützte Arbeitsmodelle vorbereiten können. Zugleich wurde uns die enorme Bedeutung einer ganzheitlichen KI-Souveränitätsstrategie bewusst, die neben den technologischen Aspekten vor allem die menschliche und ethische Dimension eines verantwortungsbewussten und produktiven Umgangs mit KI berücksichtigt.

Wenn Sie zur Wahrung der Datenhoheit zunehmend auf verteilte Edge-Geräte und dezentrale Open-Source-Modelle umsteigen, wird Ihr Netzwerk zum neuen Sicherheitsperimeter. Eine dezentrale KI-Strategie erfordert eine agile, intelligente und globale Basis. Die NaaS-Lösung (Network-as-a-Service) von Verizon basiert auf einer verwalteten Infrastruktur, die auf souveräne KI-Anwendungen ausgelegt ist. Ihre Daten werden dynamisch, sicher und präzise weitergeleitet und verarbeitet, ohne Kompromisse bei Leistung, Geschwindigkeit oder Compliance einzugehen.

In manchen Branchen sind vollständige Autonomie und KI-Souveränität keine realistischen Ziele. Für viele Unternehmen wird jedoch die Wahrung der Unabhängigkeit und die Kontrolle über proprietäre Daten zunehmend zur Priorität.



Mehr zum Thema

Unternehmen weltweit stehen vor der drängenden Frage, wie sie mit KI-Souveränität Mehrwert schaffen und ihr Netzwerk auf die entsprechenden Anforderungen ausrichten. Verizon unterstützt sie dabei, mithilfe von KI Innovationsprozesse zu beschleunigen,

ihr Serviceangebot auszubauen, Erkenntnisse zu gewinnen und Business-Intelligence-Prozesse zu optimieren. Erfahren Sie, was wir für Ihr Unternehmen tun können.

