

Sonderdruck aus  
BI-Spektrum 3/2025



Bild: suldev, stock.adobe.com

Zwischen Innovation, Kosten und Sicherheit

# Daten- und KI-Souveränität

Ein Beitrag von  
Johannes Wenzel,  
Frank Ballert und  
Enrico Gabriele

Daten und KI treiben die Wertschöpfung moderner Unternehmen, doch ihre Nutzung verlagert sich – gerade in Bezug auf den Einsatz von KI – zunehmend in die Cloud. Aus diesen Abhängigkeiten ergeben sich Risiken, die vor dem Hintergrund der aktuellen geopolitischen Situation eine neue Brisanz erlangen. Damit wird die Frage der Souveränität über Daten und KI-Anwendungen zu einem strategischen Wettbewerbsfaktor. Im Artikel wird gezeigt, wie durch eine ausgewogene Balance zwischen Innovationskraft, Kosten und Souveränität die langfristige Unabhängigkeit und Handlungsfähigkeit im Unternehmen sichergestellt werden kann.

Der Trend der wachsenden Komplexität von Lieferketten, der in den 2010ern in der Fertigung begann, hat in den letzten zehn Jahren zunehmend auch die Data & Analytics-Welt erfasst. Die Einführung immer neuer Werkzeuge, der Umzug von Datenplattformen in die Cloud, die Verwendung von Software as a Service (SaaS) und die Einbeziehung immer neuer Datenquellen schaffen Abhängigkeiten, die gravierende Auswirkungen auf die Nutzbarkeit von Daten und den Einsatz von KI haben können.

Daher wird die Daten- und KI-Souveränität zunehmend wichtiger: Inwieweit kann das Unternehmen über alle Aspekte der Speicherung, Verarbeitung und Nutzung von Daten selbst bestimmen? Wie können Daten rechtssicher, geschützt und ohne externe Einschränkungen genutzt werden? Die Beantwortung dieser Fragen ist entscheidend, um die Resilienz der Datenverarbeitung zu gewährleisten, Mehrwerte aus Daten und KI zuverlässig zu heben und das Vertrauen von Kunden sowie Geschäftspartnern zu stärken. Die Souveränität von



Abb. 1: Treiber der Daten- und KI-Souveränität

[zum Inhalt](#)

Daten und KI wird damit zum strategischen Thema, das im Schnittpunkt zwischen Daten- und KI-Strategie auf der einen und IT-Strategie auf der anderen Seite betrachtet werden muss.

## Steigende Relevanz der Daten- und KI-Souveränität

Zwei Treiber erhöhen aktuell die Relevanz der Souveränität: die geopolitische Lage und neue rechtliche und regulatorische Anforderungen, die überwiegend von der EU vorangetrieben werden (Abbildung 1).

In Bezug auf die geopolitische Lage spielen die zunehmenden protektionistischen Tendenzen und politischen Unsicherheiten eine wesentliche Rolle, die Auswirkungen auf die Verfügbarkeit und Kosten von SaaS-Angeboten haben können. In Bezug auf rechtliche und regulatorische Anforderungen sind insbesondere die Datenschutz-Grundverordnung (DSGVO) mit Bezug zu personenbezogenen Daten, NIS-2 bei Kritischen Infrastrukturen, DORA im Finanzbereich und der Cyber Resilience Act bei Herstellern und Händlern von „smarten“ Produkten zu nennen.

KI sowie Data & Analytics sind aufgrund der für Analyse, Training und Tuning erforderlichen großen und häufig sensiblen Datenmengen besonders stark von der Frage der Daten- und KI-Souveränität betroffen. Vorgaben zur Datenresidenz und die Notwendigkeit kurzer Übertragungswege zwischen Datenspeicherung und -verarbeitung, insbesondere mit GPUs, erhöhen die „Data Gravity“ und binden Modelle, Pipelines und Workloads an konkrete Plattformen. Hinzu kommen proprietäre Daten-, Modell- und MLOps-Formate, die eine Portabilität erheblich erschweren.

Bei der Adoption von KI durch Unternehmen sind dabei zwei Tendenzen zu beobachten. Viele Unternehmen nutzen die KI-Angebote der Hyperscaler, bei denen ihre Daten bereits liegen, und erhöhen damit die Abhängigkeiten massiv. In anderen Unternehmen gibt es eine Art von „Wild-West“-Kultur: Der erste KI-Provider, welcher der IT oder einem Fachbereich geeignet erscheint, wird ausgewählt. Oft nutzt man sogar mehrere Anbieter für gleichartige Anwendungen im selben Unternehmen. Eine Prüfung, ob und wie sich solche Sourcing-Entscheidungen auf die Souveränität auswirken, wird selten vorgenommen.

## Souveränität mit Augenmaß als Schlüssel zur digitalen Selbstbestimmung

Eine vollständige Daten- und KI-Souveränität ist oft schwer oder gar nicht zu erreichen. Gründe für eine Entscheidung zu Abstrichen in der Souveränität können vielfältig sein (siehe Abbildung 2). Dabei müssen die Aspekte der Souveränität wie Schutz der Daten, Portabilität, externe Einflussnahme oder Kosten-Risiken (siehe Tabelle 1) gegen die Wirtschaftlichkeit abgewogen werden, insbesondere in Bezug auf:



**DR. JOHANNES WENZEL** ist Chief Information Security Officer bei INFOMOTION und berät Unternehmen im Rahmen der Management-Beratung zu Datenstrategien und Informationssicherheit. Mit langjähriger Erfahrung in Plattformarchitekturen, Data- und Analytics-Systemen sowie Security-Themen unterstützt er Organisationen dabei, ihre Datenlandschaften sicher und zukunftsfähig zu gestalten.  
**E-Mail: Johannes.Wenzel@infomotion.de**

**FRANK BALLERT** verfügt über langjährige Erfahrung im Data & AI-Umfeld, von der Planung und dem Design über die Entwicklung bis hin zur Administration von Data Warehouses, Data Lakes, Data Lakehouses und Data Meshes inklusive AI-Anwendungen in unterschiedlichsten Unternehmensbereichen. Als Solution Architect für Data & AI bei der STACKIT nutzt er diese Erfahrung, um Kunden bei ihren Vorhaben zu unterstützen, souveräne Data & AI-Lösungen umzusetzen und Mehrwerte zu schaffen.

**E-Mail: frank.ballert@stackit.cloud**

**ENRICO GABRIELE** ist Head of Data & AI Consulting bei STACKIT, dem souveränen Cloud-Anbieter der Schwarz Gruppe. Er blickt auf über ein Jahrzehnt Erfahrung zurück, in dem er Unternehmen entlang der gesamten Data, Analytics & AI-Wertschöpfungskette strategisch und operativ begleitet hat.

**E-Mail: enrico.gabriele@stackit.cloud**

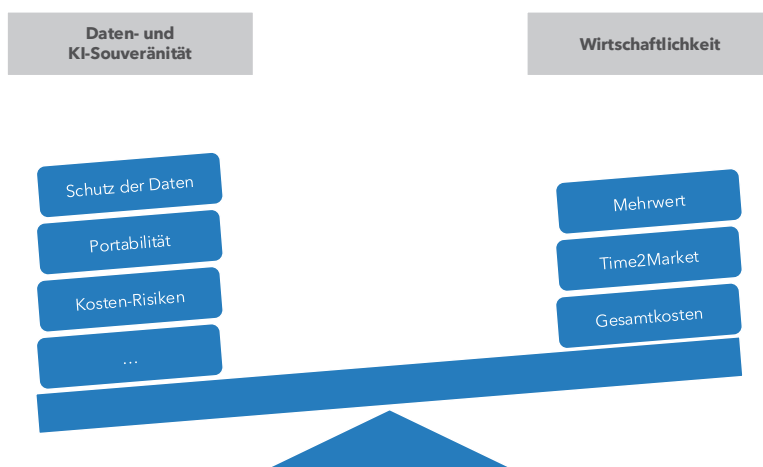


Abb. 2: Daten- und KI-Souveränität im Spannungsfeld

[zum Inhalt](#)

Aspekt	Klasse der Daten- und KI-Souveränität		
	Hoch	Mittel	Gering
<b>Schutz der Daten</b>	Speicherung, Übertragung und Verarbeitung On- Premises oder mit kundenspezifischer Verschlüsselung ausschließlich im Inland	Speicherung, Übertragung und Verarbeitung mit EU-spezifischer Verschlüsselung ausschließlich innerhalb EU/EWR	Speicherung und Verarbeitung innerhalb EU/EWR, Netzwerk (zum Beispiel Content Delivery) auch außerhalb EU/EWR möglich
<b>Rechtsprechung und Einflussnahme</b>	Rechtsprechung ausschließlich im Inland, kein ausländischer Einfluss zur Dateneinsicht oder Verfügbarkeit von Diensten möglich	Rechtsprechung ausschließlich in EU/EWR, kein Einfluss zur Dateneinsicht oder Verfügbarkeit von Diensten außerhalb EU/EWR möglich	Rechtsprechung ausschließlich in EU/EWR
<b>Portabilität</b>	Daten, Modelle und Anwendungen portabel (zum Beispiel Open-Source-Formate und -Anwendungen)	Daten und KI-Modelle portabel	Daten und KI-Modelle exportierbar
<b>Betriebsverantwortung</b>	Verantwortung für alle Prozesse des Betriebs im Unternehmen oder mit Rückfallmöglichkeiten in den Betrieb (oder im Unternehmen) im Rahmen tolerierbarer Ausfallzeiten	Einflussmöglichkeiten des Unternehmens auf alle Prozesse des Betriebs (zum Beispiel Auslieferung von Updates/Patches, Möglichkeiten eines Rollback)	Dokumentierte Schnittstellen und Verantwortlichkeiten im Rahmen des Betriebs
<b>Auditierbarkeit</b>	Zertifikate und Audits können im Detail nachvollzogen werden. Alle Prozesse können zusätzlich eigenständig auditiert werden.	Zertifikate und Audits können im Detail nachvollzogen und zur Erfüllung regulatorischer Anforderungen durch eigene Auditierungen ergänzt werden.	Zertifikate von Auditierungen sind einsehbar.
<b>Kostenrisiko</b>	Langfristige Planungssicherheit für Kosten hinsichtlich Herstellerkosten und Handelsabgaben	Langfristige Planungssicherheit für Herstellerkosten ODER Handelsabgaben	Eingeschränkte Planungssicherheit bei Herstellerkosten und Handelsabgaben

**Tab. 1:** Klassen der Daten- und KI-Souveränität (exemplarisch)

- **Mehrwert für das Business:** Erhöhung des Umsatzes durch neue oder erweiterte Geschäftsmodelle oder durch Einsparungen durch Steigerung der Effektivität oder Effizienz.
- **Geschwindigkeit:** Verbesserung der „Time-to-Market“ durch die Nutzung der Service-Angebote (zum Beispiel von Spezial-Anbietern oder Hyperscalern) können Datenprojekte gegebenenfalls schneller und effektiver umgesetzt werden als durch eine Realisierung mit hoher Souveränität (zum Beispiel Eigenentwicklung), insbesondere wenn wenig KI-Know-how im eigenen Unternehmen vorhanden ist.
- **Gesamtkosten:** Kosten zur Umsetzung von Daten- und KI-Use-Cases einschließlich der Kosten zur Herstellung des gewünschten Grads an Daten- und KI-Souveränität. Hierbei ist auch die Aufteilung in initiale und fortlaufende Kosten relevant.

Diese Abwägung sollte risikoorientiert erfolgen. Wie dies genau geschieht, wird im Folgenden beschrieben. Die Risikoorientierung kann auch beinhalten, dass für bestimmte Phasen (zum Beispiel während der Evaluation eines Use-Case) ein höheres Risiko akzeptiert wird als für den produktiven Betrieb.

Dabei ist es sinnvoll, im Unternehmen Souveränitätsklassen festzulegen, die eine einfache Zuordnung je nach Bedeutung der Geschäftsanwendung für das Unternehmen zulassen. Tabelle 1 zeigt eine solche Einteilung in Souveränitätsklassen, die gemäß den Anforderungen des Unternehmens angepasst werden müssen.

Die Abwägung, welche Souveränitätsklasse an welcher Stelle notwendig ist, kann für verschie-

dene Anwendungen durchaus unterschiedliche Ergebnisse liefern. So kann zum Beispiel für geschäftskritische Anwendungen ein höherer Grad an Souveränität notwendig sein als für unterstützende Anwendungen.

## Besonderheiten für Daten und KI am Beispiel von generativer und agentischer KI

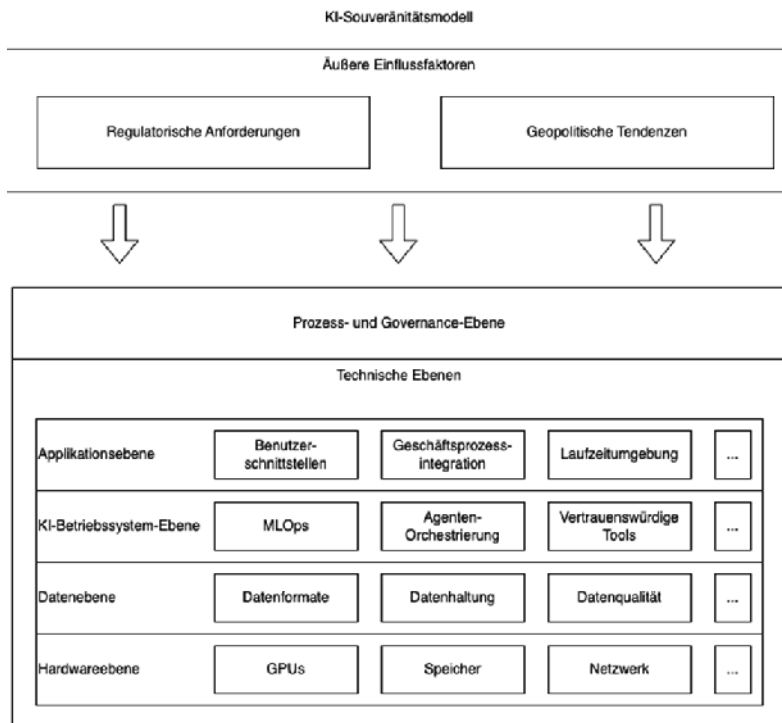
Der Datenbedarf für generative und agentische KI steigt beständig: Schätzungen zeigen, dass hierfür notwendige Large Language Models zwischen 2026 und 2028 alle öffentlichen verfügbaren Daten in ihrem Training verwenden werden – über 1,3 Quadrillionen Wörter [Vil24]. Diese verwendeten Daten sowie die Entscheidungen, die KI-Agenten auf deren Basis treffen, stellen zusätzliche signifikante Herausforderungen für ein angemessenes Souveränitätsniveau dar:

1. **Abhängigkeit von LLMs und deren Werten:** KI-Agenten basieren häufig auf LLMs, die immense Datenmengen und Rechenressourcen für Training und Bereitstellung erfordern. Hier stellt sich die kritische Frage, ob die Trainingsdaten nationale und lokale Gegebenheiten wie Kultur und Unternehmenswerte adäquat widerspiegeln [Mar20]. Geschieht dies nicht, kann ein KI-Agent andere Werte vertreten als das eigene Unternehmen.
- **Tool-Zugriff und -Verkettung** [Bug25]: Das Model Context Protocol (MCP) und das Agent2Agent Protocol (A2AP) vereinfachen die Entwicklung von KI-Agenten und Multi-Agenten-Systemen zunehmend. MCP ermöglicht bei-

spielsweise die standardisierte Integration von Tools wie zum Beispiel Suchmaschinen und eine Warendispositionssoftware [Ant25; Sur25]. Dies kann zur Entwicklung äußerst leistungsfähiger, aber auch potenziell riskanter KI-Agenten führen. Ohne ein entsprechendes Design könnte ein KI-Agent beispielsweise entscheiden, sensible Informationen aus einem Dokumentenmanagementsystem für eine Websuche zu nutzen. Das gefährdet nicht nur die Datenkontrolle und somit die Souveränität, sondern birgt auch das Risiko, gegen regulatorische Vorgaben zu verstoßen (zum Beispiel DSGVO) [ViH25].

2. **Autonome Entscheidungsfindung und Handeln:** KI-Agenten treffen teilweise oder vollständig autonome Entscheidungen und handeln entsprechend – oft ohne direkte menschliche Aufsicht [YaR25]. Der Einsatz eines nichtsoveränen KI-Agenten birgt das Risiko, die Kontrolle über kritische Entscheidungen und Aktionen an Akteure abzugeben, die potenziell anderen Jurisdiktionen oder Normen unterliegen. Ein Beispiel verdeutlicht dies: Wenn ein KI-Agent zur Warendisposition im Lebensmittelgroß- und -einzelhandel eingesetzt wird und seine Schnittstelle zur Warenwirtschaftssoftware aufgrund von Exportbeschränkungen abgeschaltet wird, kann das negative Auswirkungen auf die Versorgungssicherheit der Bevölkerung haben.

3. **Workflow-Erinnerung und Kontextmanagement** [Bug24]: Hat ein KI-Agent erfolgreiche Routinen gelernt, kann er diese speichern und wiederverwenden, was man als Workflow-Erinnerung bezeichnet [Wan24]. Hinzu kommt das Kontextmanagement, das LLMs und KI-Agenten dazu befähigt, in einem bestimmten Kontext die richtigen Entscheidungen (wahrscheinlicher) zu treffen. Die Kontrolle darüber ist demnach bedeutend für domänenspezifische Adaptationen,



die Erklärbarkeit von Entscheidungen und welche Routinen gelernt werden.

Abb. 3: KI-Souveränitätsmodell

Diese Herausforderungen und die potenziellen Risiken unterstreichen die Wichtigkeit eines risikobasierten Ansatzes für KI-Systeme, wie der des EU AI Act. Ein risikobasiertes Vorgehen ermöglicht auch, bewusste Entscheidungen für mehr KI-Souveränität zu treffen. Um dem auf allen Ebenen zu begegnen, wird daher ein KI-Souveränitätsmodell (siehe Abbildung 3) vorgestellt, das die kritischen Dimensionen von der Hardware bis zur Governance zusammenfasst:

- **Hardwareebene:** Beinhaltet technische Hardwarekomponenten von GPUs, TPUs, ASICs

**SIGS.DE**  
 sigs.de  
 Fachinhalt zu Software-Architektur, Development, Java, Künstlicher Intelligenz, Analytics und weitere Schwerpunktthemen  
 Informationsdienste · Iroisdorf, Nordrhein-Westfalen · 141 Follower:innen  
 Nachricht + Folgen

Follow us now on  
**Linked in**

zum Inhalt

QR code with 'SCAN ME' button and a vertical stack of social media icons (hearts, thumbs up).

Tab. 2: Handlungsoptionen von Unternehmen

Ebene des KI-Souveränitätsmodells	Handlungsoption
Prozess- und Governance-Ebene	Formulierung einfacher und verständlicher Regeln zum Einsatz von KI sowie deren Einbettung in bestehende Governance-Frameworks und ISMS (zum Beispiel COBIT, ISO 27001, ISO 42001)
Applikationsebene	Transparente Darstellung der Nachvollziehbarkeit von KI-Entscheidungen sowie eine API-basierte und modulare Entwicklung, um Austauschbarkeit und Portabilität zu gewährleisten
KI-Betriebssystem-Ebene	Einsatz von Open-Source-Software und -Modellen zur Entwicklung (zum Beispiel e5-mistral-7b-instruct, LangGraph, mlflow) sowie Erstellung eines eigenen Registers vertrauenswürdiger Tools für KI-Agenten
Datenebene	Verwendung von offenen Datenformaten (zum Beispiel Apache Iceberg), Open-Source-Datenbanken und kundenverwalteten Schlüsseln zur serverseitigen Datenverschlüsselung in Cloud-Umgebungen
Hardwareebene	Nutzung souveräner Private-, Hybrid-, Public- und Multi-Cloud-Ansätze und -Angebote (zum Beispiel STACKIT), Air Gapping sowie Hardware-Sicherheitsmodule zur Verwaltung von kryptographischen Schlüsseln

(Application Specific Integrated Circuit) über Speicher und deren Bezugsquellen bis hin zu Rechenzentrumsstandorten und der benötigten Elektrizität.

- **Datenebene:** Hierzu zählen Aspekte wie die verwendeten Datenformate, die Datenherkunft, der Ort der Datenhaltung sowie die Qualität und Repräsentativität der Daten.
- **KI-Betriebssystem-Ebene:** Umfasst alle Komponenten des MLOps (wie Entwicklungsumgebung, Workflow-Orchestrierung, Modelltraining etc.) [KKH23] sowie zusätzliche Komponenten, die durch KI-Agenten erforderlich werden (zum Beispiel ein Tool-Register für die Integration vertrauenswürdiger Tools).
- **Applikationsebene:** Betrifft die Endanwendung, in welche die KI integriert wird, inklusive ihrer Schnittstellen, des Nutzerinteraktionsdesigns und der Bereitstellungsumgebung.
- **Prozess- und Governance-Ebene:** Beinhaltet Aspekte wie die Festlegung von Verantwortlichkeiten, Auditierbarkeit, Compliance mit rechtlichen und ethischen Rahmenbedingungen (zum Beispiel EU AI Act, EU Data Act), Risikomanagement und die Gestaltung von menschlicher Aufsicht bei autonomen Systemen.

## Handlungsoptionen von Unternehmen

Das vorgestellte Modell kann von Unternehmen als Framework zur systematischen Bewertung der kritischen Ebenen ihrer KI-Systeme zugrunde gelegt werden, um ein angemessenes Souveränitätsniveau zu erreichen. Ohne auf die Vorteile moderner KI-Systeme zu verzichten, müssen Unternehmen demnach gezielte Entscheidungen treffen. Im Folgenden werden daher wichtige Handlungsoptionen

für Unternehmen aufgeführt, die es ihnen ermöglichen, digitale Selbstbestimmung zu sichern und dabei die Balance zwischen Innovation, Kosten und Sicherheit zu finden.

Die Liste an möglichen Handlungsoptionen ist lang. Sie beginnt bei Themen wie der Versorgung von Hardware mit Elektrizität und erstreckt sich bis hin zum Know-how-Aufbau bei Mitarbeitenden. Daher werden in Tabelle 2 ein paar der wichtigsten Bereiche dargestellt. Diese ermöglichen es, den angemessenen Grad an Souveränität gezielt auf jeder der fünf Ebenen umzusetzen und bieten eine Inspiration für weitere, auch unternehmens- und branchenspezifische Optionen. Denn: Dass Souveränität mehr als Kontinuum zu sehen ist und alle Optionen ebenfalls unterschiedliche Ausprägungsstufen je nach Kritikalität mit sich bringen, wird bereits aus Tabelle 1 klar ersichtlich.

## Vorgehen zum Erreichen der optimalen Daten- und KI-Souveränität

Wie oben dargestellt, ist eine gute Governance für Daten und KI eine wichtige Voraussetzung, um eine optimale Daten- und KI-Souveränität zu erreichen. Dabei zeigt die Erfahrung, dass Governance-Ansätze, die auf Fähigkeiten und Kompetenzen aufsetzen, bessere Ergebnisse erzielen als regel-/policyzentrierte Ansätze. Eine gute Daten- und KI-Souveränität profitiert damit sowohl von einer „gelebten“ Governance für Daten und KI als auch von Awareness für die besonderen Anforderungen der Souveränität.

Konkret basiert die Ermittlung der derzeitigen und notwendigen Daten- und KI-Souveränität immer auf einer Analyse der Geschäftsprozesse, bei der die Kritikalitäten [BSI08] der jeweiligen Prozes-

Abb. 4: Vorgehen zur Bestimmung der notwendigen Daten- und KI-Souveränität



se und Teilprozesse ermittelt werden (siehe Abbildung 4). Danach müssen alle Anteile der oben beschriebenen Ebenen (Daten, Hardware etc., kurz „Assets“), die in den jeweiligen Geschäftsprozessen relevant sind, ermittelt und dem entsprechenden Prozess zugeordnet werden. So kann der Grad der Kritikalität der jeweiligen Assets präzise ermittelt werden.

Die ersten Schritte (hell dargestellt in Abbildung 4) sind identisch mit den im Rahmen des Business Continuity Management (BCM) notwendigen Aktionen. Daraus wird ersichtlich, dass die Verbesserung der Daten- und KI-Souveränität optimalerweise mit dem BCM, das ein notwendiger Bestandteil jedes Informationssicherheitsmanagement-Systems (ISMS) ist, kombiniert werden kann. Insgesamt sollten alle hier beschriebenen Schritte konsequent im Rahmen des ISMS und nicht als getrennter Prozess umgesetzt werden.

Aufbauend auf der Ermittlung der Kritikalität können anschließend die Souveränitätsklassen entsprechend zugeordnet werden: Eine hohe Kritikalität erfordert in der Regel auch eine hohe Souveränität! Dabei sollten sowohl die derzeit vorhandene Souveränitätsklasse als auch die gewünschte beziehungsweise notwendige Souveränitätsklasse ermittelt werden. In Zweifelsfällen kann durch eine zusätzliche Risikobetrachtung ein höheres Maß an Sicherheit für die Entscheidung, welche Souveränitätsklasse gewählt werden muss, gewonnen werden.

Fast alle Hyperscaler bieten ergänzende Maßnahmen, die auf die Erhöhung der Daten- und KI-Souveränität einzahlen können. Diese reichen von der Gründung europäischer Tochterunternehmen über das Angebot verschiedener Service-Levels bis hin zur „Customer-Managed Keys“-Verschlüsselung, die eine externe Einsichtnahme verhindert. Diese ergänzenden Maßnahmen sollten bei der Planung von Maßnahmen zur Herstellung der gewünschten Souveränitätsklasse berücksichtigt werden.

Auf Basis der Ergebnisse aus den vorherigen Schritten kann in der Folge ein Migrationsplan entwickelt werden. Hierbei sollten die größten Abweichungen in der Ist- gegen die Soll-Souveränität zuerst behandelt werden. Gegebenenfalls sind Überlegungen zur Vereinheitlichung genutzter Services oder Plattformen (insbesondere mit Bezug zu KI) sinnvoll. Natürlich müssen bei der sich so ergebenden „Souveränitäts-Roadmap“ auch verfügbare Ressourcen und die entsprechende Kostenplanung einbezogen werden.

## Fazit

Das Erreichen eines hohen Grads an Daten- und KI-Souveränität ist kein Selbstläufer – auch nicht in Unternehmen mit einem gut etablierten und funktionierenden Informationsmanagement-System.

Gerade in Bezug auf Daten und KI stellen sich komplexe Herausforderungen. Je reifer die Daten- und KI-Strategie ist und je besser die Governance für Daten und KI ausgeprägt ist, desto einfacher kann die Souveränität gesteuert werden. Echte souveräne Public-Cloud-Angebote wie STACKIT werden immer mehr verfügbar und fördern diesen Trend zusätzlich.

Dabei gibt es kein „One Size Fits All“. Jedes Unternehmen muss seine eigenen Ziele in Bezug auf die Daten- und KI-Souveränität selbst festlegen und die notwendigen Schritte zur Erreichung dieser Ziele umsetzen. Dabei sollten die Aspekte der Souveränität sowohl auf strategischer Ebene bei Entscheidungen in Bezug auf Daten und KI als auch auf taktischer Ebene in Bezug auf die schnellen Entwicklungszyklen und die vielfältigen Verknüpfungsmöglichkeiten agentischer KI berücksichtigt werden. Zudem ist es sinnvoll, die Entwicklung nicht ausschließlich auf Basis von Prozessen und Vorgaben voranzutreiben, sondern frühzeitig auf Kompetenzen und Awareness für das Thema zu setzen.

## Literatur

- [Ant25] Anthropic: Introducing the Model Context Protocol. 25.11.2024, <https://www.anthropic.com/news/model-context-protocol>, abgerufen am 4.8.2025
- [BSI08] Bundesamt für Sicherheit in der Informationstechnik: BSI Standard 100-4. In: BSI-Standard 100-4 – Notfallmanagement. Bonn 2008, S. 100ff.
- [Bug25] Bughin, J.: The Real AI Battle: OS is the New Prize. 18. Juli 2025, <https://www.europeanbusinessreview.com/the-real-ai-battle-os-is-the-new-prize/>, abgerufen am 4.8.2025
- [KKH23] Kreuzberger, D. / Kühl, N. / Hirschl, S.: Machine Learning Operations (MLOps): Overview, Definition, and Architecture. IEEE Access, Bd. 11, 2023, S. 31866-31879
- [Mar20] Martin, A.: Wie können wir unsere Expertise auf europäischer Ebene nutzen, um die europäische KI-Souveränität zu sichern? 23.11.2020, <https://www.iis.fraunhofer.de/de/magazin/serien/kuenstliche-intelligenz-ki-serie/european-sovereignty-in-ai.html>, abgerufen am 4.8.2025
- [Sur25] Surapaneni, R. et al.: Announcing the Agent2Agent Protocol (A2A). 9.4.2025, <https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interopability/>, abgerufen am 4.8.2025
- [ViH25] Vineeth, N. S. / Habler, I.: Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies. 11.4.2025, <https://arxiv.org/html/2504.08623v2>, abgerufen am 4.8.2025
- [Vil24] Villalobos, P. et al.: Position: will we run out of data? limits of LLM scaling based on human-generated data. In: International Conference on Machine Learning, Wien 2024
- [Wan24] Wang, Z. Z. et al.: Agent Workflow Memory. 11.9.2024, <https://arxiv.org/html/2409.07429v1>, abgerufen am 22.8.2025
- [YaR25] A. Yazdanbakhsh, A. / Reddi, V. J.: Architecture 2.0: Foundations of Artificial Intelligence Agents for Modern Computer System Design. In: Computer, Bd. 58, 2025, S. 116-124