

Digitale Souveränität

**Konkrete Handlungsoptionen
statt Symboldebatte**

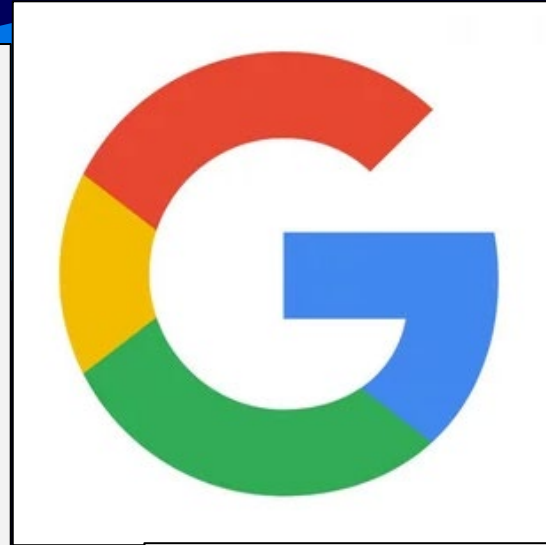
Dr. Thomas Götz

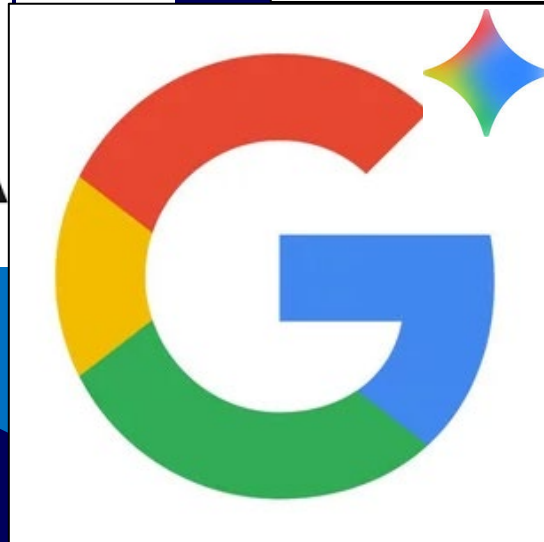
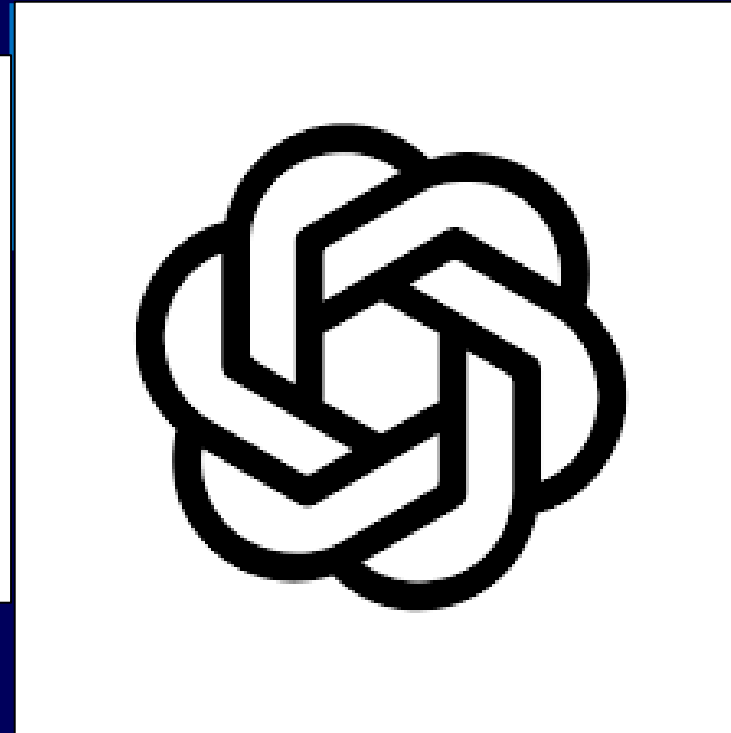
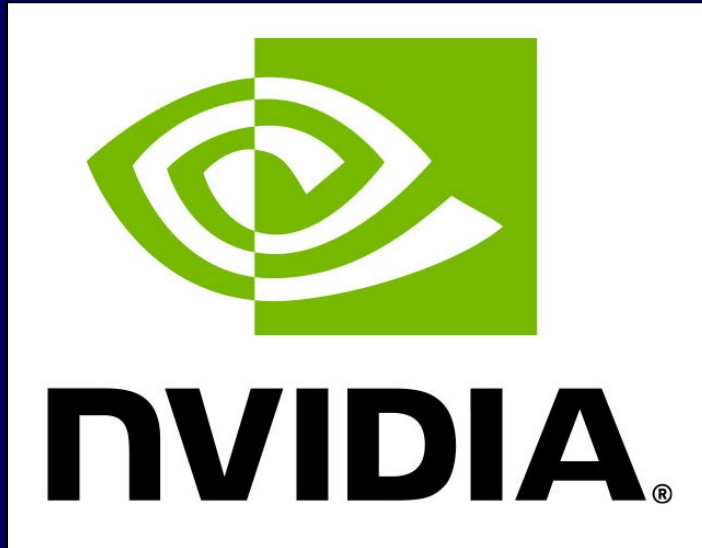
CTO and Head of Innovation Management

Atos Germany, Austria, Central Europe



Atos





Marktanteile der Cloud- und KI-Hyperscaler

Wie gehen Entscheider mit der Machtkonzentration der marktbeherrschenden IT- und KI-Anbieter um ?

85 %

„Marktanteil“ der fünf führenden Anbieter von KI-Modellen
im Jahr 2026 artificialanalysis.ai/

75 %

Marktanteil der drei führenden Cloud-Hyperscaler im Jahr 2026

Synergy Research Group

35 %

Durchschnittlicher Anstieg der tatsächlichen Kosten für digitale Plattform-Services seit 2022

<https://www.silicon.de/41717852/kostenfalle-microsoft-Cloud>

0,5 – 10
Mio. €

Change-Kosten beim Versuch, die digitale Plattform zu wechseln

<https://www.hfsresearch.com/research/strategic-hyperscaler-contracts-buyers-remorse/>

70

Prozentualer Anteil der IT-Entscheidungsträger, die der Ansicht sind, dass ein Wechsel zwischen den großen digitalen Plattformen (Cloud, KI) realistisch nicht durchführbar ist

BCG-Analyse: 500 befragte IT-Entscheidungsträger, „Managing the evolving dynamics of digital platform lock-in“, BCG, 7. November 2025

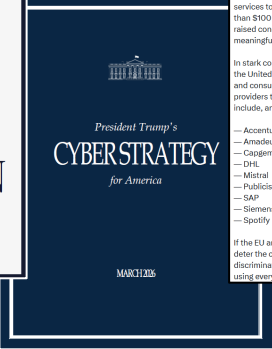
12
Std

Durchschnittliche jährliche Ausfallstunden bei großen Cloud-Hyperscalern seit 2023

IX 01/2026

Neue Realitäten in der Debatte um die (KI-)Souveränität

Regionale Industriestrategien, Vorschriften, Compliance-Rahmenwerke, Gesetzgebung zum extraterritorialen Datenzugriff



United States Trade Representative @USTTradeRep

The European Union and certain EU Member States have persisted in a continuing course of discriminatory and harassing lawsuits, taxes, fines, and directives against U.S. service providers. U.S. services companies provide substantial free services to EU citizens and reliable enterprise services to EU companies, and they support millions of jobs and more than \$100 billion in direct investment in Europe. The United States has raised concerns with the EU for years on these matters without meaningful engagement or basic acknowledgement of U.S. concerns.

In stark contrast, EU service providers have been able to operate freely in the United States for decades, benefitting from access to our market and consumers on a level playing field. Some of the largest EU service providers that have hitherto enjoyed this expansive market access include, among others:

- Accenture
- Amdocs
- Capgemini
- DHL
- Mistral
- Publicis
- SAP
- Siemens
- Spotify

If the EU and EU Member States insist on continuing to restrict, limit, and deter the competitiveness of U.S. service providers through discriminatory means, the United States will have no choice but to begin using every tool at its disposal to counter these unreasonable measures.

16.12.2025

„[...] es ist für die Vereinigten Staaten aus Gründen der nationalen Sicherheit unerlässlich, eine unangefochtene und unbestrittene globale technologische Vorherrschaft zu erlangen und aufrechtzuerhalten.“ (Donald J. Trump, 10.7.2025) – „Americas AI Action Plan“



Chinese
Cybersicherheitsgesetze, Änderung tritt am 1. Januar 2026 in Kraft
Die Novelle unterstreicht Chinas Unterstützung für Forschung und Entwicklung im Bereich Schlüsseltechnologien wie Artificial Intelligence („KI“)



EU AI Act

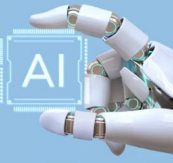
Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

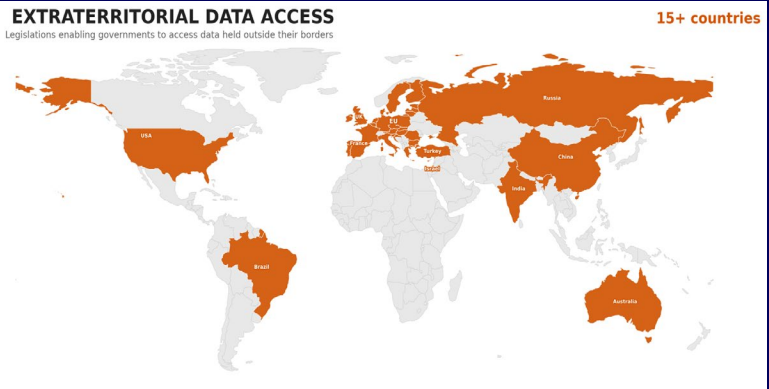
2021/0106 (COD)

European Commission



InvestAI initiative







Atos

Die neue Realität

Die vier zentralen Entscheiderfragen zum Stand digitalen Souveränität

- Die sich selbst verstärkende **Dominanz** des **Plattformmodells** für digitale Services
- Das Ende der multilateralen **Weltordnung** mit offenen Handelsbeziehungen
- Die Nutzung **technologischer Abhängigkeiten** als Mittel zur Erpressung
- **Geopolitische Fragmentierung** in Regionen mit unterschiedlichen Werten und Rechtssystemen
- Auswirkungen technologischer Entscheidungen auf **die Wahrnehmung** von Unternehmen oder **deren Wettbewerbsfähigkeit**



Kann ich die digitale Plattform * auf die ich mich gerade abstütze, jederzeit verlassen?



Habe ich jederzeit Zugang zu den erforderlichen wettbewerbsrelevanten Technologien? Welche Möglichkeiten habe ich?



Habe ich (und nur ich) jederzeit Zugriff auf meine wichtigsten geschäftskritischen Daten und Metadaten?



Bewege ich mich in einem auch zukünftig stabilen rechtlichen Rahmen, der eine Planung ermöglicht?

Umgang mit kritischen Abhängigkeiten

Welche kritischen Abhängigkeiten sind akzeptabel ?

Vorteile aus Nutzung von Assets mit kritischen Abhängigkeiten

- **Innovationsfähigkeit** (R&D Ausgaben, API Spektrum)
- **Markteinführungszeit** (Cloud DevSecOps und PaaS)
- **Skalierbarkeit** (Cloud-Rechenleistung, Speicher, Netzwerk, ...)
- **Flexibilität** (Services/APIs: Breite und Tiefe)
- **Qualität** (LLMs, ...)



- Anwendungen (Methoden, Algorithmen, Modelle)
- Daten (Rohdaten, Trainingsdaten, ...)
- Infrastruktur (Rechenzentren, Netzwerke, ...)
- Vertragliche Rechte, Lizenzen, ...
- Fachwissen (Quellen, Zugang)

- **Komplexität** (große Anzahl von Stacks und Technologien)
- **Cybersicherheit** (laufende Updates erforderlich)
- **Supply Chain** (Lieferanten-, sBOM- und Kategorie-management)
- **Fachkräfte** (Verfügbarkeit, Lernkurve)

KI-bezogene Ressourcen

Inferenzumgebung: digitale Infrastruktur, Daten, Modelle, Anwendungen, Software, Middleware, Systeme, Hardware und Betrieb

Trainingsdatensätze: Herkunft, Inhalt, Integrität und Lebenszyklusmanagement, die die Effizienz, Robustheit und Verzerrungen des Modells beeinflussen

Unsere Definition von digitaler Souveränität

Digitale Souveränität ist eine Fähigkeit – wir nennen sie „Managed Sovereignty“



Management kritischer Abhängigkeiten

Digitale Souveränität ist die Fähigkeit, kritische Abhängigkeiten entlang der gesamten digitalen Wertschöpfungskette der IT selbstbestimmt und proaktiv zu managen



Differenzierter Schutz, Management und Kontrolle

Digitale Souveränität erfordert daher einen differenzierten Schutz, ein differenziertes Management und eine differenzierte Kontrolle geschäftskritischer Technologie-, Daten- und Anwendungs-Assets über das gesamte Spektrum unterschiedlicher Souveränitätsanforderungen hinweg.



Kontinuum verfügbarer Optionen

Voraussetzung für diese Fähigkeit ist die Bereitstellung eines Kontinuums flexibel einsetzbarer Technologie-Stacks und Werkzeuge für Infrastruktur, Daten und Anwendungen – als Optionen, die jederzeit für die optimale Platzierung von Daten und Workloads zur Verfügung stehen.

Die vier Dimensionen der Souveränität

Souveränität erfordert das bewußte, selbstständige Setzen von Prioritäten

Unabhängiges
Handeln ohne
externe Kontrolle
(„kein Kill-Switch“)

Autonomie

Resilienz

Geschäftskontinuität
trotz unerwünschter
Ereignisse

Vermeidung von
unerwünschten
Ereignissen

Sicherheit

Kontrolle

Wirksame
Durchsetzung von
Entscheidungen
und Regeln

Gestaltungsoption für eine höhere KI-Souveränität

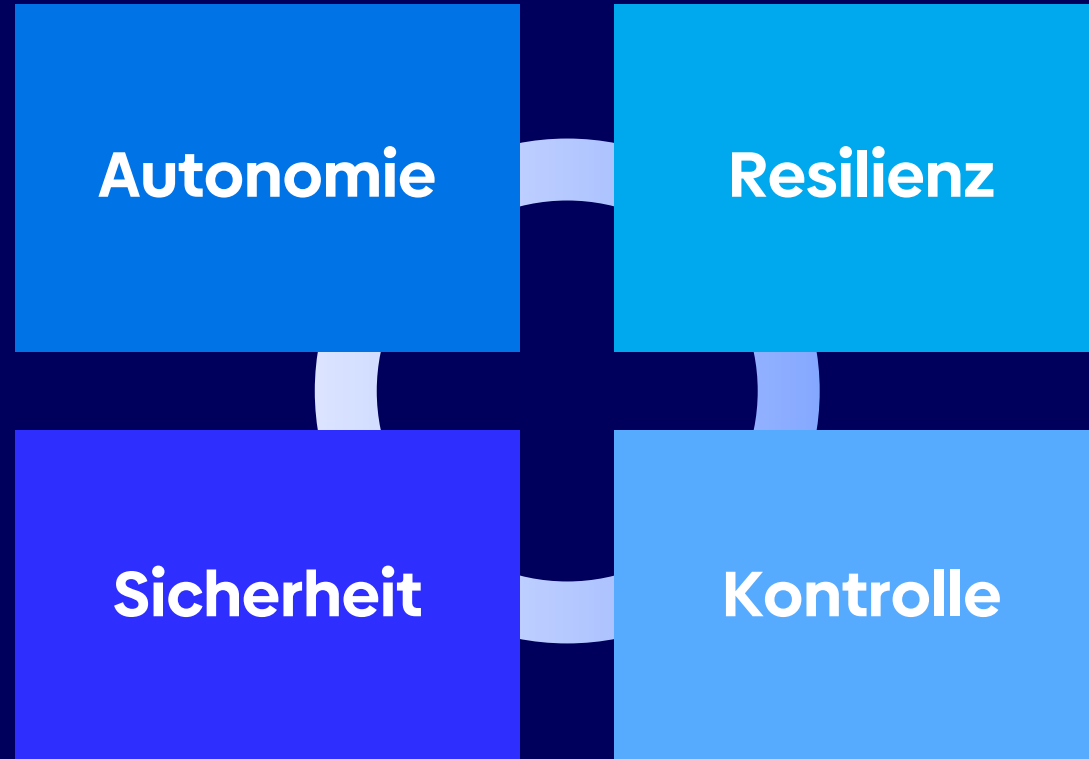
Wichtige „Design Choices“ für eine souveränere KI

„Kill-Switches“ vermeiden

- Modellauswahl und Modellgröße
- Auswahl der Infrastruktur/Technologie einschließlich AI Supply Chain
- Deployment-Optionen
- Portabilität / Alternativen

Angriffsvektoren abwehren

- Agentensicherheit und Identitäten
- Modellierung adversarischer Angriffe
- Datenmanipulation und -vergiftung
- Datenlecks / Datenextraktion
- Kuratiertes API-Management



Robuste Implementierung

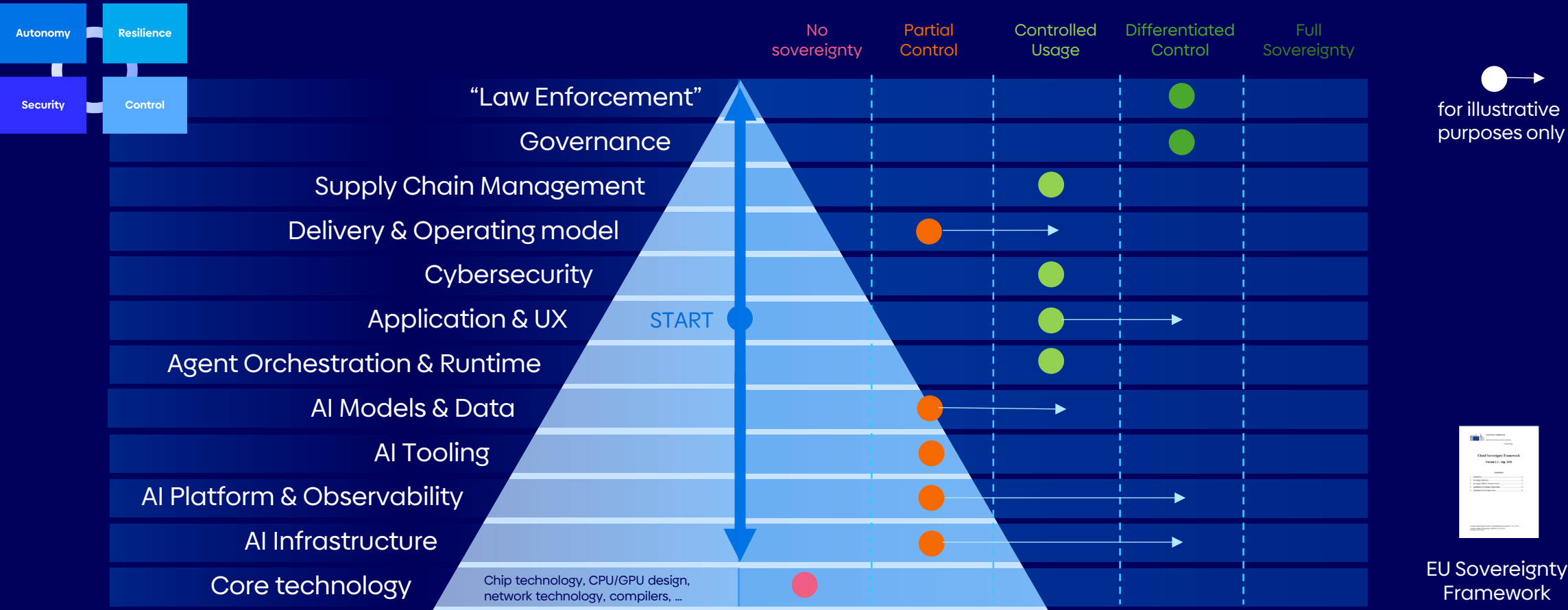
- HA/DR-Architektur
- Technische Beobachtbarkeit
- Beobachtbarkeit von KI-Verhalten

„Safety Belts“ einziehen

- « Control Plane »
- KI-Governance
- Kostenbeobachtbarkeit (FinOps)
- Erklärbarkeit von KI
- Einhaltung gesetzlicher Vorschriften
- HITL-Regeln und -Abläufe

Realistische Zielniveaus für erhöhte Souveränität

Systematisches Vorgehen für alle Assets mit kritischen Abhängigkeiten



Atos AI Sovereignty Framework © 2025, compliant with EU Cloud Sovereignty Framework Version 1.2.1 – Oct. 2025

Souveränitätsziele im Rahmen des Machbaren

Die Managed AI Sovereignty Scorecard – Ein KPI-basierter Ansatz



Hebel zur Stärkung der Fähigkeiten für „Managed Sovereignty“

Hebelwirkung



Größere
Transparenz



Flexible
Architektur



Stack
Umschaltung



Zielgerichtete
Diversifizierung



Fokussiert
Open Source



Mehr
Redundanz

Technologieoptionen

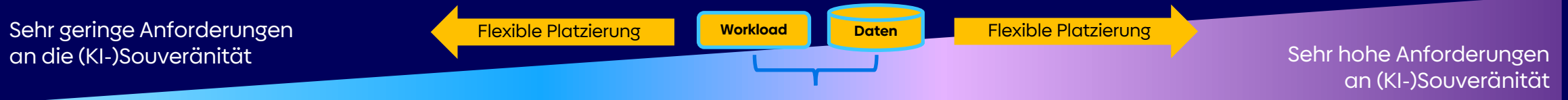
- End-to-End-Stückliste („BOM“) der Asset-Supply Chain → **kritische Abhängigkeiten schnell identifizieren und verstehen**
- Reduzierte Integration und verstärkte Modularisierung der Architektur → **Schnellerer und risikoärmerer Austausch und Migration kritischer Komponenten**
- Plattform-/Cloud-Migration → **Auswahl besser kontrollierbarer Anbieter**
- Diversifizierung von Technologien und Plattformen → **Risiken streuen, breiteres Fachwissen erhalten**
- Gezielter Einsatz von Open Source → **Verringerung kritischer Anbieterabhängigkeiten**
- Redundanz für die kritischsten Komponenten und Anbieter → **Erhöhung der Ausfallsicherheit**

Anpassung des IT-Betriebsmodells

- Regelmäßige, differenzierte Kosten-Nutzen-Analyse pro Asset in Abstimmung zwischen IT und Geschäftsbereichen
- Aktive Überwachungsfunktion über die gesamte IT-Service-Kette hinweg für jede kritische Ressource (Basis SW BOM und HW BOM)
- Verbesserte Folgenabschätzung und **strategische Leitlinien** hinsichtlich der Auswahl und Nutzung digitaler Plattformen
- Geeignete Orchestrierungs-, Betriebs- und Kontrollmodelle für plattformübergreifende und Multi-Stack-IT
- Aktive Einflussnahme auf Anbieter, Integratoren und Partner durch Co-Innovation von Features
- **Vertragliche Regelung** von Flexibilitäten und Optionen für Changes und Reversibilität

Atos Sovereign IT & AI Continuum – „Managed Sovereignty“ für unsere Kunden

Differenzierte Steuerung für alle Daten- und Workload-Assets, kombiniert mit flexibler Nutzung geeigneter Technologie-Stacks pro Asset über das gesamte Spektrum der Souveränitätsanforderungen hinweg.



Souveränitäts-Management- und Steuerungsebene

Management der Anforderungen an die KI-Souveränität

Kostenmanagement (FinOps & TBM)

Management der IT-Richtlinienkontrolle und -durchsetzung (Nutzung, Durchsetzung, Compliance, Governance, Automatisierung)

IT-Cybersicherheitsmanagement (Identitäts- und Zugriffsmanagement, souveräner SOC-Betrieb, Erkennung und Reaktion auf Bedrohungen, Verschlüsselung)

Management von Multi-Agenten Systemen (Orchestrierung, Beobachtbarkeit, Sicherheit, Isolierung, Robustheit, Vorhersagbarkeit, Erklärbarkeit, Überprüfbarkeit)

Application Management (Personal, konforme Anwendungsarchitektur, API, Stückliste, Supply Chain, Open Source, Integrierbarkeit, Interoperabilität)

Datenmanagement (Personal, konforme Datenplattformarchitektur, API, Stückliste, Supply Chain, Open Source, Datenportabilität)

Asset-Management (Codes & Workloads, KI-Modelle, KI-Evaluierungen, Datensätze – zentralisiert, dezentralisiert, föderiert – einschließlich Backup-Strategien)

Infrastruktur für Souveränität (Atos-Rechenzentren, Kundenrechenzentren, Partnerrechenzentren, EU-/DE-Superscaler, Hyperscaler)

Multi-Stack-Infrastruktur-Orchestrierung und Steuerungsebene (Abstraktion, Integration, IaaS, PaaS, Workload-/Datenverlagerung, Automatisierung)

Native

Globale Public-Cloud-/SaaS-Lösungen
„wie vorgefunden“

Kontrolliert

Public-Cloud-/SaaS-Lösung
ergänzt durch souveräne Kontrollen

Vertrauenswürdig

lokale / zertifizierte Lösung
ergänzt durch souveräne Kontrollmechanismen

“Disconnected”

Air-Gapped-/Offline-/Private Varianten

Digitale Souveränität

Conclusio

1. Erhöhte Digitale Souveränität ist in der neuen Realität ein **zentrales Anliegen** für alle Unternehmen und Organisationen.
2. Digitale Souveränität ist eine **Fähigkeit**, die man trainieren muss, und kein Zustand.
3. **Autonomie, Sicherheit, Resilienz und Kontrolle** sind die Säulen digitaler Souveränität, und sind bewusst, proaktiv, kontinuierlich und konsistent zu gestalten.
4. Die **Souveränität von KI**, insbesondere von agentischer KI, ist entscheidend für souveräne digitale Operationen.
5. Souveränität von KI und agentischer KI sind nicht zu trennen, sondern **KI führt zu einer neuen Kritikalität von Abhängigkeiten** über alle Ebenen der IT.
6. Der Aufbau der Fähigkeit digitaler Souveränität ist **nichts für einsame Alleingänge**.