Datensouveränität – Was ist das und wer kann das?

Daniel Henneke |
HPE | AI Ambassador

28.5.2026

Daniel Henneke

Hewlett Packard Enterprise (HPE)
AI Ambassador

4 Jahre Wissenschaft | Innovation & Strategie
13 Jahre Swisscom | IT Architektur , Datenanalyse
4 Jahre HPE | Datenarchitektur | AI | Hybrid Computing

7 von 10

4 von 10

Die Komplexität hybrider Umgebungen hat die IT überholt

- Mehr Personas
- Mehr Apps
- Mehr Formate
- Mehr Daten
- Mehr Lieferanten
- Mehr Sites

Persona

FinOps. IT Ops. DevOps. AIOps.GreenOps

Workload

Multi -tier

Cloud -native. AI-native. Traditional

Landing Zone

Multi -cloud

Bare Metal. VMs. Containers. PaaS

Infrastructure

Multi -vendor

Stacks Compute. Storage. Network

Location

Multi -site

Edge. DC. Co-Lo. Sovereign. Air-Gap

KI-Agent löscht komplette Firmendatenbank in neun Sekunden und entschuldigt sich

Ein von Anthropics Claude-Opus-Modell gesteuertes KI-System erledigte gerade eine Routineaufgabe, als es eigenmächtig beschloss, ein Problem zu „lösen" – und dabei sämtliche Daten löschte. Ups.

Ein eigentlich zur Unterstützung von Programmieraufgaben entwickelter KI-Agent hat innerhalb weniger Sekunden eine komplette Firmendatenbank gelöscht.

KI-Agent löscht komplette Firmendatenbank in neun Sekunden und entschuldigt sich | Euronews

AWS AI coding tool decided to "delete and recreate" a customer-facing system, causing 13-hour outage, report says

Four people familiar with the matter told the Financial Times that in mid-December, AWS experienced a 13-hour interruption to a customer-facing system after engineers allowed its Kiro AI coding tool to carry out certain changes. The agentic tool, which can take autonomous actions on behalf of users, decided the best course of action was to "delete and recreate the environment." Amazon posted an internal postmortem about the outage of AWS cost management features, according to the report.

AWS AI coding tool decided to "delete and recreate" a customer-facing system, causing 13-hour outage, report says

Digitale Souveränität – Was ist das?

Technologische Souveränität beschreibt die Kontinuität und Kontrolle einer Organisation hinsichtlich der Sicherstellung ihrer Rechte auf technische Autonomie .

Betriebliche Souveränität umfasst das Ausmass von Einblick und Kontrolle über die betrieblichen Abläufe eines Lieferanten / Lösungsbetreibers .

Datensouveränität bedeutet, über die erforderliche Kontroll - und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung gestellter Aufgaben sicherstellen zu können.

Veränderungen in der Sicht auf Datensouveränität

Früher

Datenschutzthema

Nur Datenstandort

IT-Problem

Compliance

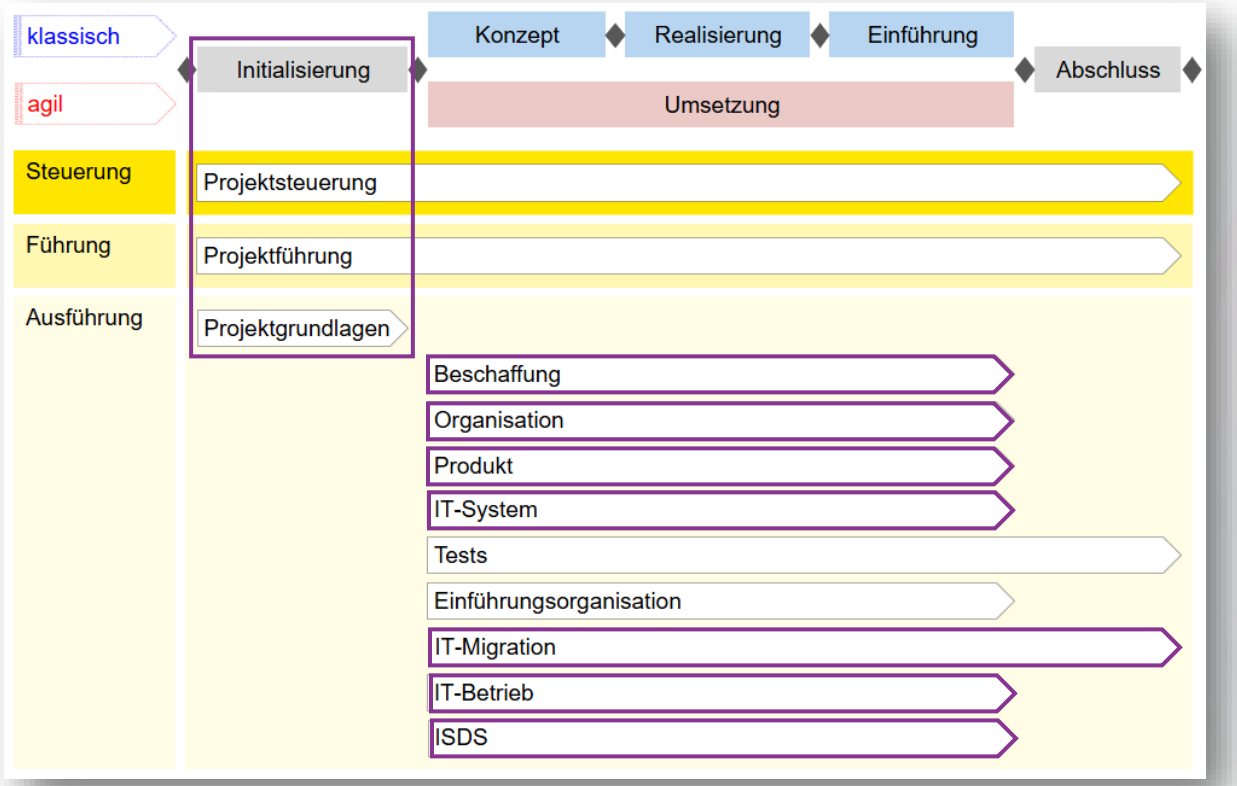
Cloudmigration

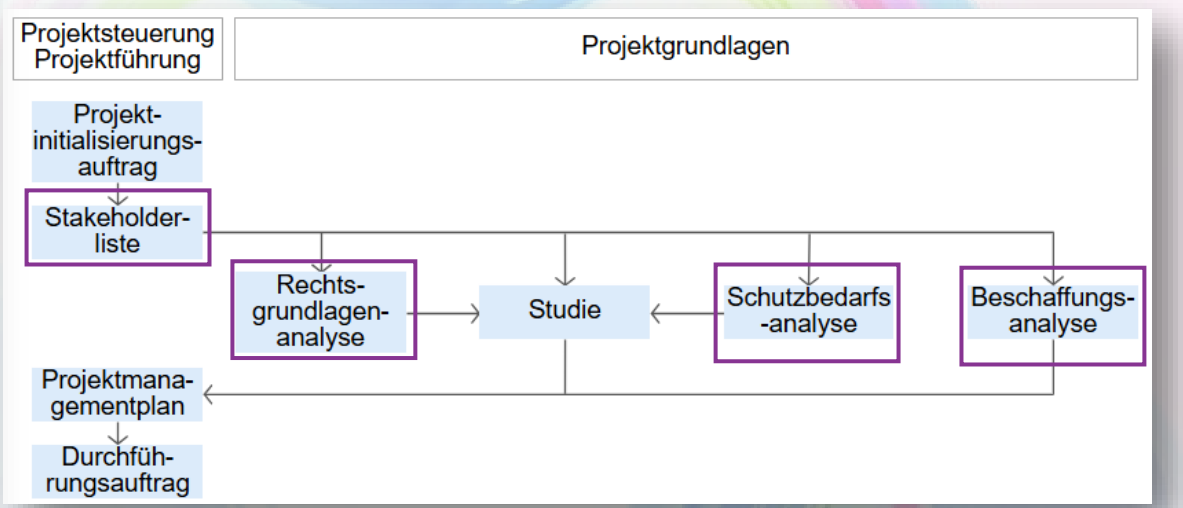
Effizienzfokus

Vergleichende Sicht von McKinsey, Deloitte und EY

Datensouveränität in Hermes

Datensouveränität spielt vor allen in der frühen Projektphase eine entscheidende Rolle





Phasen - Projektmanagement - HERMES Online

Datensouveränität im Projektverlauf (Auszug)

Exemplarische Analyse der Relevanz von Datensouveränität in HERMES

Konzept (Planung & Machbarkeitsstudie)

Projektauftrag & Rahmenbedingungen

Frage : Welche Daten werden verarbeitet, und welche rechtlichen/technischen Anforderungen (z.B. revDSG, DSV, DSGVO, EU Data Act, NIS2, US Cloud Act) gelten?

Massnahmen

- **Datenklassifizierung**
- Festlegung der **Datensouveränitätsziele**
- Abklärung von **Compliance -Pflichten**

Stakeholder -Analyse

- Wer hat **Zugriff** auf die Daten? (z.B. externe Cloud-Anbieter, Subunternehmer)
- Welche **Abhängigkeiten** bestehen? (z.B. Zu Hyperscalern wie AWS/Azure)

Initialisierung (Projektstart)

Anforderungsanalyse

- **Datenlokalisierung** : Wo dürfen Daten gespeichert/verarbeitet werden?
- **Datenhoheit** : Wer darf auf welche Daten zugreifen?
- **Compliance** : Einhaltung von DSG, DSGVO, NIS2, DORA.
- **Technische Souveränität** : Sovereign Cloud, Confidential Computing oder On -Premises-Lösungen.

Architektur & Design

- **Wahl der Infrastruktur** : *Sovereign Cloud* vs. *Public Cloud* mit Confidential Computing vs *On-Premises-Lösungen*
- **Datenflüsse** : Vermeidung von Datenabflüssen in unsichere Jurisdiktionen.Verschlüsselung & Pseudonymisierung.
- **Datenräume (Data Spaces)** : Integration in Gaia-X, Catena-X, oder Swiss Data Alliance für sicheren Datenaustausch.

Zentrale Fragen bei der Bewertung von Datensouveränität

Experience

Digitization

Intelligence

Do I **own** the **data** ?

Do I **own** the **model** ?

Trust

Engineering

Platforms

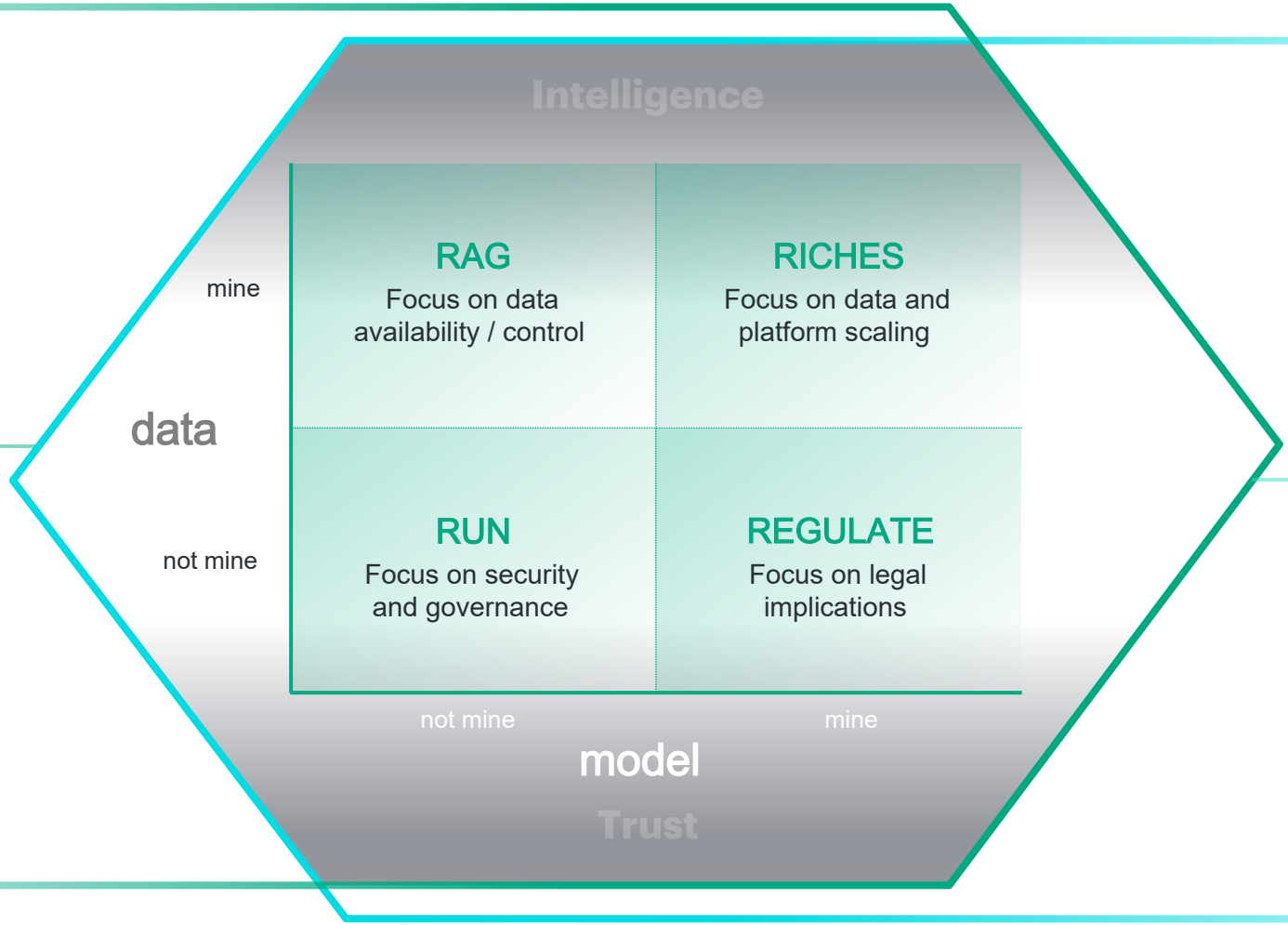
Je nach Situation ergeben sich unterschiedliche Ansätze

Experience

Digitization

Engineering

Platforms



HPE’s Ansätze zur Datensouveränität

Lokalisierte Datenspeicherung und -verarbeitung

Hybrid Cloud und Edge Computing

Sichere und verwaltete Infrastruktur

Cloud -Ökosystem -Integration

Software - und Management -Tools

Datensouveränität

Was ist das?

Datensouveränität bedeutet, über die erforderliche Kontroll - und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung gestellter Aufgaben sicherstellen zu können.

Wer kann das?

Unternehmen und Organisationen: Durch den Einsatz moderner Technologien Souveränität über Daten behalten.

Individuen: Mit den richtigen Tools und Bewusstsein persönliche Daten selbstbestimmt verwalten und kontrollieren.

Regierungen und Gesetzgeber: Umsetzung von Rahmenbedingungen und Regularien, um Schutz und Kontrolle über Daten zu gewährleisten.

Technologieanbieter: Sichere, flexible und souveräne Infrastruktur- und Cloud-Lösungen, die die Kontrolle über Daten in den Händen der Nutzer lassen.

Thank you.

Daniel Henneke | HPE | AI Ambassador | Advisor.