

SKW Schwarz

iapp

# Digital Sovereignty in Practice

## What European Cloud Standards Actually Deliver

**IAPP European Privacy KnowledgeNet 12.10.2026**

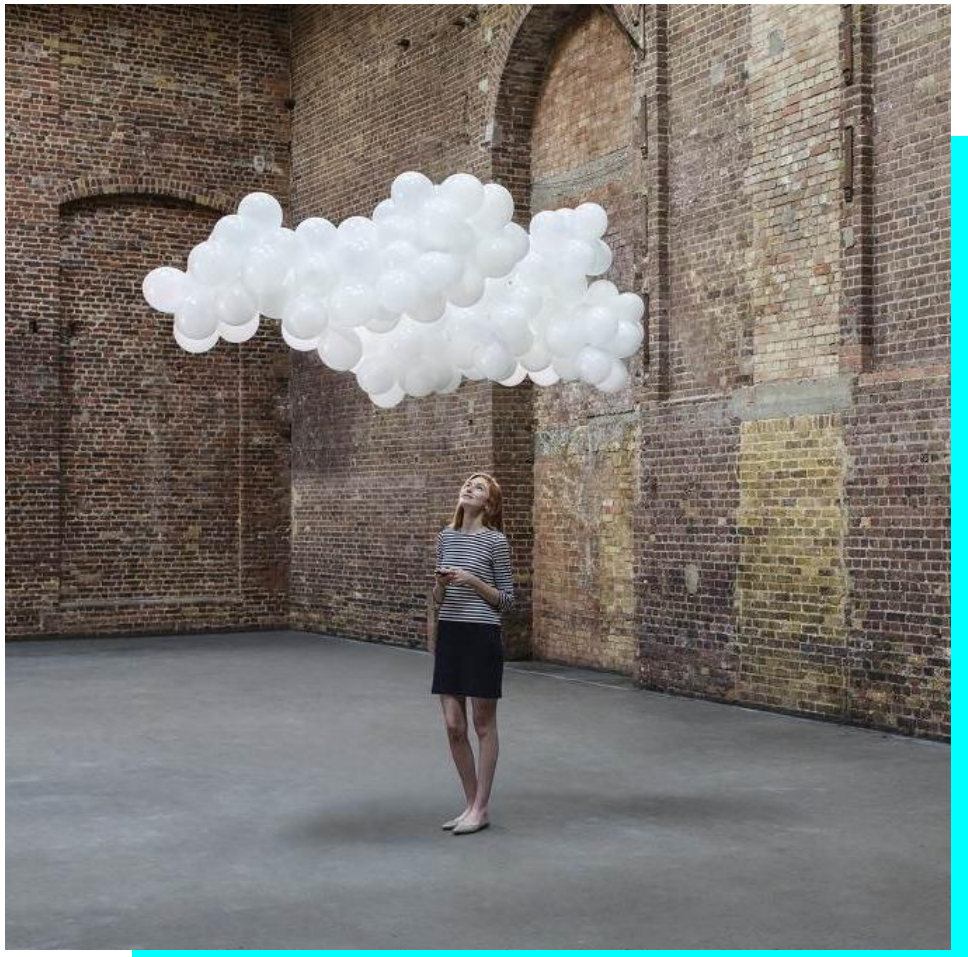
Dr. Matthias Orthwein, LL.M. (Boston)

# 01

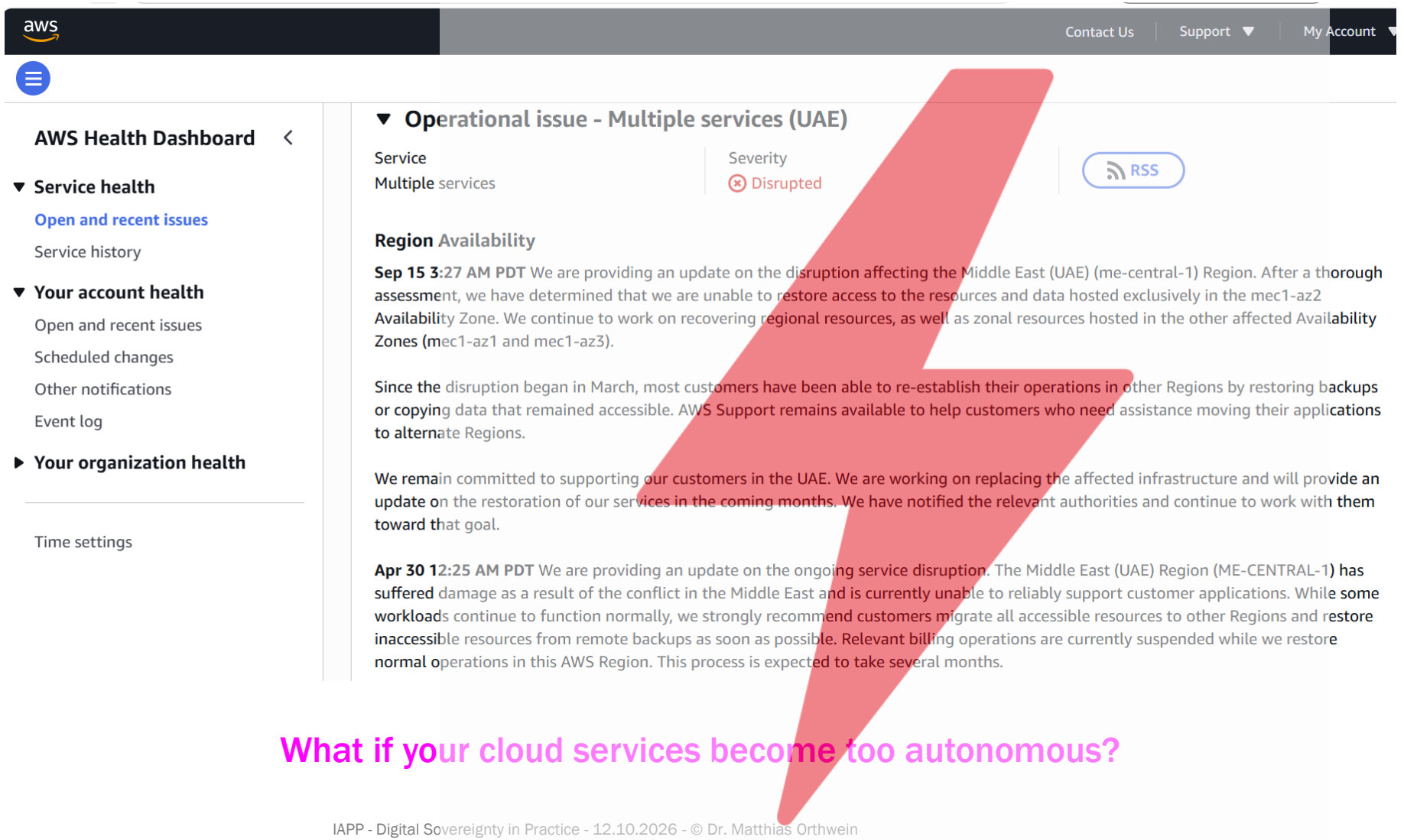
# Digital Sovereignty - the Concept and Challenges

# Why Digital Sovereignty Matters Now

- → European customers increasingly demand control over data, operations and legal exposure.
- → Cloud choices are no longer only about price and performance, but also about jurisdiction, resilience and independence.
- → **Digital Sovereignty** may not be understood as technological autarky, but as the **ability to make informed and self-detemined choices**.
- → Autonomous cloud may increase your resilience by reducing your flexibility.



# Sovereignty vs. autarky




**What if your cloud services become too autonomous?**

# From Compliance to Control:

## What “Cloud Sovereignty” Really Means

- → **Sovereignty** goes beyond GDPR compliance: it is about who can actually control or disrupt your digital services.
- → **EU Cloud Sovereignty Framework** (October 2025, including implementation guideline) as guideline for assessment of sovereignty, defining eight objectives:
  - SOV1: Strategic Sovereignty
  - SOV2: Legal Sovereignty,
  - SOV3: Data & AI Sovereignty,
  - SOV4: Operational Sovereignty,
  - SOV5: Supply Chain Sovereignty,
  - SOV6: Technology Sovereignty,
  - SOV7: Security & Compliance Sovereignty,
  - SOV8: Sustainability.
- → **Autonomy** is the freedom to decide at your discretion about the “if”, “where” and “how” of data processing and about granting or denying access to your data.

# Why Digital Sovereignty Matters

Six drivers: control over data, operations and the freedom to exit

### 1 Data & AI under control

Sovereign cloud is a way to practically implement **GDPR** principles of control, accountability and security.

GDPR · SOV 3

### 2 Cyber resilience by law

**NIS2, CRA and DORA** require risk management, incident reporting, supply-chain security and **business continuity**.

NIS2 · CRA · DORA

### 3 Staying online under stress

EU-only admins and EU-based support keep services running despite support withdrawal, **geopolitical disruption** or foreign export restrictions.

SOV 4

### 4 Protecting trade secrets

**R&D and IP „crown jewels“** keep their value only while secret. Fully controlled operations limit foreign leverage and espionage risk.

Trade Secrets Directive · NDAs · SOV 2 & 5

### 5 Portability & sovereign exit

**Switching rights** call for open standards, standard APIs, export formats and documented exit plans = freedom to make decisions.

EU Data Act · SOV 4, SOV 6

### 6 Public sector & defence ready

Tenders, **export controls and national security** rules demand that critical and classified workloads remain under exclusive EU control.

Public tenders · export control

Legal basis: GDPR · NIS2 · Cyber Resilience Act · DORA · Trade Secrets Directive (EU 2016/943) · EU Data Act · export control & national security rules

# CADA: Europe's Cloud and AI Development Act

## Strategic Context

- → **CADA** (proposed in June 2026, **not yet enacted**) aims to strengthen the EU's cloud and AI ecosystem by increasing domestic capacity and reducing dependence on non-EU hyperscalers.
- → It introduces a single EU-wide sovereignty framework under **8 explicit operational objectives** with specific auditable criteria and assurance levels for cloud services.
- → For European IT providers, CADA is both a business opportunity and a road map for future compliance expectations.
- → DORA supply chain requirements for financial industry will not be replaced but come on top



EUROPEAN
COMMISSION

Brussels, 3.6.2026
COM(2026) 502 final

2026/0138 (COD)

Proposal for a

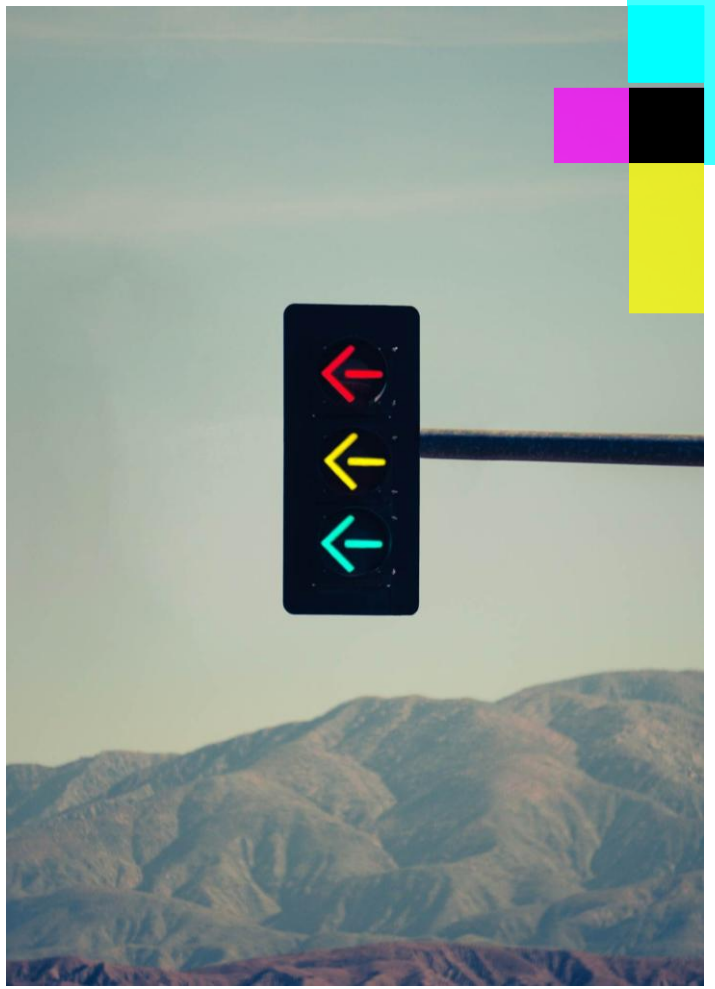
**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)**

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

# CADA Cloud Assurance Levels: SEAL 1 to 4

- → **4 cloud assurance levels** define increasing degrees of sovereignty: from basic EU establishment (Level 1) to fully EU-controlled stack and supply chain (Level 4).
- → Public sector and critical NIS2 sectors will be mapped (within 2 years from enactment) to required levels, making assurance levels a **central purchasing criterion**.
- → Public sector customers can only purchase services with the correct SEAL according to their mapping
  - Only exception: even **second** public tender requiring this SEAL failed to produce a suitable provider
- → **Scope**: personal data as well as any confidential or sensitive information; delivery of AI systems (not the model or system provision)
- → **Localisation Geography**: EU-wide, not necessarily one dedicated EU-country



# CADA Cloud Assurance Levels: SEAL1 to 4

**SEAL1**

- Data is processed and stored in infrastructure located in the EU
- Provider is not forced to disclose not-yet-exploited software vulnerabilities to any non-EU government

**SEAL2**

- Data may not be used to train AI-models operated in non-EU countries and may not leave the EU
- No third country has the ability to disrupt the service
- Full transparency over software supply chain

**SEAL3**

- EU ownership/control of the provider
- EU-only personal
- 3rd country providers may be accepted by EU Commission

**SEAL4**

- Full EU-control over all assets, services and supply chain
- No interference from 3rd countries possible
- European cybersecurity certificate of at least “high” assurance level

# CADA Requirements:

## What Providers Must Show in Practice

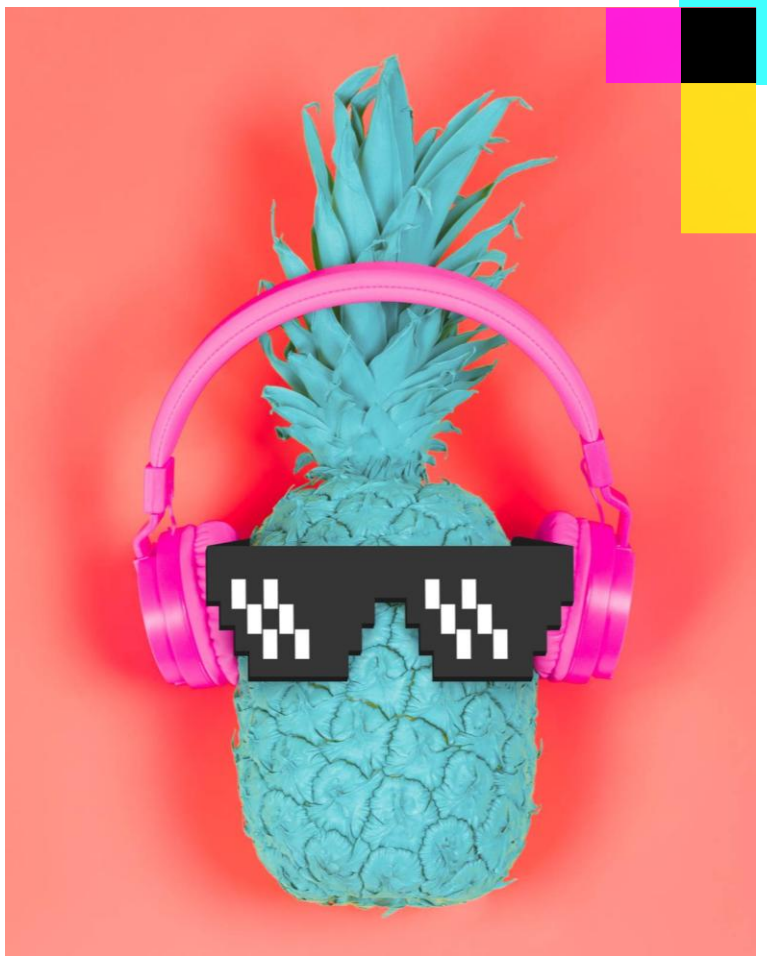
→ **Criteria** for SEAL assessment:

- EU establishment,
- Location of infrastructure, assets and personal (including citizenship),
- data localization,
- AI systems operated by a third country,
- Technical and operational support provided outside the EU,
- absence of third-country access,
- robust cybersecurity posture and transparent software supply chain.

→ Level 1 relies on **self-declaration**; Levels 2–4 require **independent audits** and **recognition of the Member State's regulator**.

→ Chose your appropriate sovereignty level: Not every workload needs SEAL4, but critical and regulated workloads typically require SEAL2 or higher

→ EU commission will publish a **central repository of recognized providers**



# Challenges to Digital Sovereignty

Sovereignty = the freedom to make self-determined and informed decisions

| | Risk | What happens | Self-determined? | Informed? |
|---|---|---|---|---|
| 1 | **Extraterritorial reach**<br>CLOUD Act · FISA 702 · SOV 2 | US law can compel US-controlled providers to disclose data wherever it is stored, e.g. via ownership or support access. | Foreign authorities, not you, decide on access to your data. | Surveillance under FISA 702 happens outside your view. |
| 2 | **Sanctions & export controls**<br>SOV 1 · SOV 5 | Sanctions or export controls can force non-EU vendors to restrict or shut down services suddenly. | Foreign governments decide whether your services keep running. | No warning, no time to assess alternatives. |
| 3 | **Commercial dependence**<br>SOV 1 | End of support, product deprecation or price changes are the vendor's business decision, not yours. | Roadmap, funding and priorities are set without your influence. | Little visibility into ownership, governance and strategic plans. |
| 4 | **Cyber incidents on non-sovereign infrastructure**<br>SOV 7 · NIS2 · DORA | Monitoring, incident response and forensics depend on non-EU entities, without full access to logs. | Others decide on incident response, with delays or legal conflicts. | Unclear who sees your security telemetry; evidence may be lost. |

Based on: US CLOUD Act · FISA 702 · sanctions & export controls · NIS2 · DORA · SOV 1, 2, 5, 7

02

# How to Secure Digital Sovereignty

# The Sovereignty Test – AWS European Sovereign Cloud

## What it provides

- → German holding entity and subsidiaries covering the entire operation (infrastructure, certificates, billing, customer contracts, SOC and personal)
- → EU nationals residing in the EU as managing directors and Advisory Board of EU citizens
- → Technical Access model Nitro System has been documented as “no gaps in the design”; contractually guaranteed
- → Offering more than 90 AWS services, including AWS Bedrock AI tool
- → Customer-managed keys outside the AWS infrastructure through KMS and External Key Store.

## What it doesn’t solve

- → No independent ownership: AWS ESC GmbH is a 100% subsidiary of Amazon.com, Inc (USA).
- → Delayed software updates and debugging.
- → Limited offerings and functionalities
- → Bedrock on AWS ESC has no access to Claude, Llama, Mistral, only Amazon Nova models.
- → Support gaps and no cross-region failover.
- → Higher price than EU-central region.

# The Sovereignty Test – Microsoft EU Data Boundaries

## What it provides

- → EU-only data localisation for storage and processing
- → Increasing stack of services (M365, Dynamics 365, most Azure services)
- → Customer lockbox as gatekeeper to support access to customer data
- → Double Key Encryption and Customer Key Encryption that Microsoft cannot decrypt without the customer's key
- → Access to managed AI models through Azure OpenAI open-weight models and fully disconnected inference (Foundry Local)
- → All GDPR required contracts available

## What it doesn't solve

- → Independent operational entity: run by Microsoft Corp.
- → No fully segregated infrastructure but layers of controls
- → Delayed software updates and debugging.
- → Not all Microsoft services available
- → Access to external AI models can trigger data leak.
- → Double Key Encryption disables data-loss prevention, co-authoring of documents and search.

# The Sovereignty Test – Google Cloud Dedicated (Thales)

## What it provides

- → All operations and customer contracts are with S3NS (Thales), an EU located providing entity with EU-only management and no non-EU controlling corporate interest.
- → Fully independent EU operated infrastructure.
- → Access to software source code on license basis from Google (12 months survivability).
- → All Support activities and maintenance is done in the EU by EU-citizens.
- → Encryption technology licensed from Google but exclusively operated, administered and controlled by EU provider.
- → EU Sovereign Standard certified (SecNumCloud).

## What it doesn't solve

- → Only limited services available (no Google Workspace) and only in France & Germany.
- → Only limited AI services and models available at the start.
- → Delayed deployment of updates and debugging.
- → Commercial and technology dependencies are not removed for availability of updates and new technology.
- → Only limited redundancy and flexibility while highly dependent from EU operator.
- → Higher price (ca. 15-20% uplift)

# Relying on Standards - SecNumCloud

## ANSSI's Legal and Operational Blueprint for Sovereign Cloud

- → Cloud security standard **based upon ISO 27001**, actual version 3.2 from 8 March 2022
- → Published and designed by the **French National Cyber Security Agency (ANSSI)**
- → Requires full independent **technical audit and authority approval**
- → Imposes strict requirements on **ownership, data residency and operational control** under EU/French jurisdiction.
  - Non-EU support is admissible but only without any technical capability to access the customer data
- → Limits **non-EU shareholdings and effective control** to prevent extraterritorial laws from reaching customer data.
  - No more than 24% of corporate shares individually and no more than 39 % in total may be held by non-EU owners
  - Non-EU shareholders must not have "industrial leadership": appointing and directing the management and corporate decisions
- → Requires **operational autonomy**: customer must retain the ability to run the services on its own capabilities or with at least two third-party providers available
- → Inspires "operator model" joint ventures where EU entities run the stack, keys and operations for true legal separation; yet, only few providers approved as of today (October 2026).

# Relying on standards - BSI C3A

## Risk-Based Autonomy Instead of Hard Ownership Bans

- → **German Federal Agency on Informationsecurity** (**BSI**) published in April 2026 a proposal for Sovereign Cloud Standard, C3A
- → Follows the **EU Cloud Sovereignty Framework** and focuses on **transparency and risk management**.
  - Provider has to disclose all non-EU legal influence, data access and data locations pertaining to its services
- → Rather than prohibiting non-EU ownership, customers shall **evaluate sovereignty across objectives** and choose their required level.
  - Non-EU access should be technologically excluded, e.g. by way of **sovereign customer controls** and **Hold Your Own Key-encryption**
  - **Confidential computing** imposed while at rest and at process
- → No Vendor log-in to ensure strategic sovereignty
  - Provider must offer **standardized API and open data formats** and may not impose any technical or commercial hurdles to data migration and cloud switching
- → May be closer to actual reality regarding availability of cloud service technology

# 03

# Decision Guidance: How Much Independence Do You Really Need?

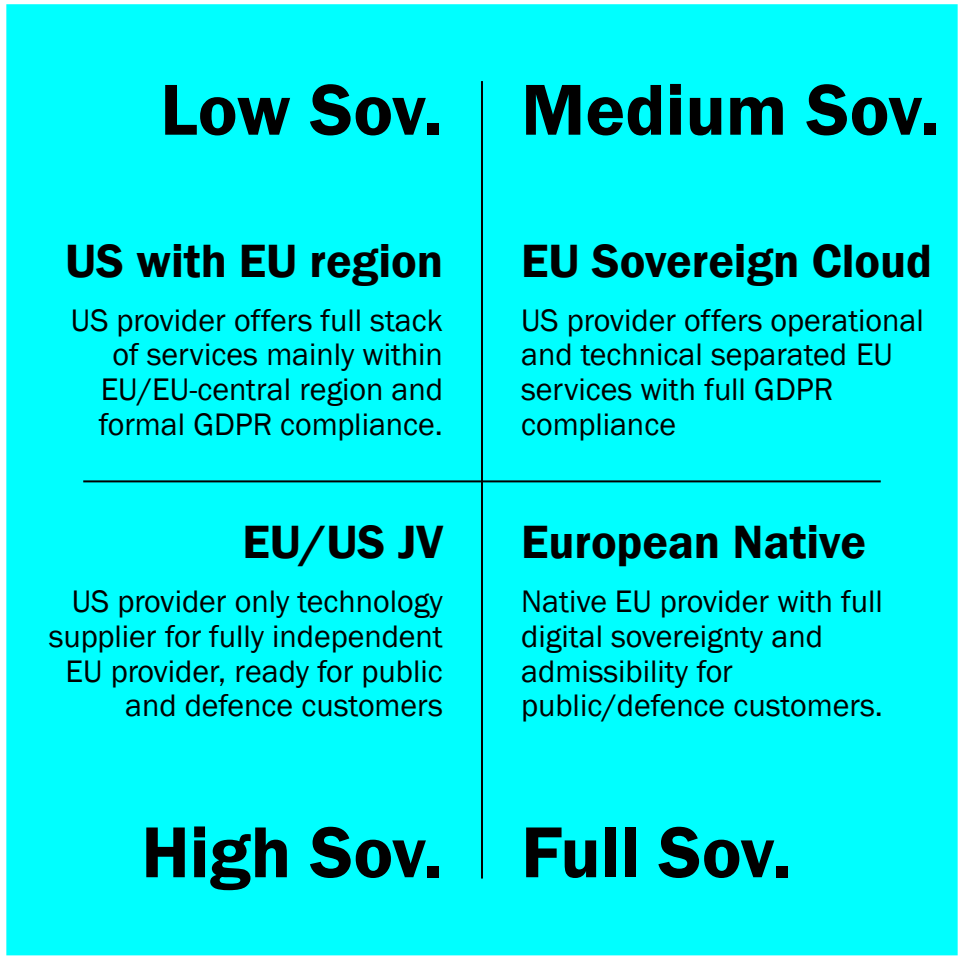
# Choose your level of Sovereignty

**Full flexibility – full non-EU exposure**

Convenient and fully flexible services including all AI models provided with a minimum level of regional focus and compliance documentation

**Limited services – legal sovereignty**

EU Joint Venture is legally and technologically sovereign but still in commercial/maintenance dependency; only limited services available and only few providers recognised.




**Increasing offerings – full GDPR/NIS2**

Full GDPR/NIS2 compliance sufficient for most commercial customers with increasing scope of services but still under US corporate control – not ready for some public and defense customers

**Fully sovereign – very limited services**

Full EU native cuts you off of new technologies and AI models; very limited services available and commercial stability of EU providers is not guaranteed.

# Additional Ressources

| | |
|---|---|
| EU Cloud Framework with implementation guide and Sovereignty Score calculator (October 2025): | https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en |
| EU Cloud and AI Development Act (CADA) (draft, EU 2026/0138, 03.06.2026): | https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada |
| SecNumCloud requirements (v3.2): | https://cyber.gouv.fr/enjeux-technologiques/cloud/ |
| BSI C3A (draft): | https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/C3A/C3A_node.html |

# Your contact for questions:




**Dr. Matthias Orthwein, LL.M. (Boston)**

Partner

+49 89 28640-102

m.orthwein@skwschwarz.de

SKW Schwarz
Wittelsbacherplatz 1
80333 Munich


Follow me on LinkedIn:
M_Orthwein


SKW
Schwarz