gart.

WHITEPAPER

Digital Sovereignty Readiness & EU Cloud Assessment Guide

A practical framework for evaluating cloud sovereignty, compliance, and EU-native cloud provider fit.

Prepared by :

Gart Solutions

Issued :

January 2026

info@gartsolutions.com

The Era of Digital Sovereignty

Europe is entering a new era of digital autonomy.

Geopolitical tensions, evolving regulatory frameworks, the rise of AI, and increased cybersecurity threats have made digital sovereignty a strategic priority for both public and private organizations.

This guide provides a practical, non-technical framework to:

- understand the pillars of digital sovereignty
- assess your organization's current sovereignty posture
- identify risks related to jurisdiction, data residency, and cloud vendor lock-in
- navigate the EU regulatory landscape
- build a modern, sovereignty-by-design cloud strategy
- evaluate EU-native cloud providers
- prepare for NIS2, Data Governance Act, Data Act, and the EU AI Act

Use this document as an internal assessment tool, a management briefing, or a checklist for cloud strategy decisions.

gart.

What Digital Sovereignty Means

Digital sovereignty refers to the ability of a nation, organization, or individual to control its own digital infrastructure, data, technology choices, and critical digital processes without dependency on external jurisdictions.

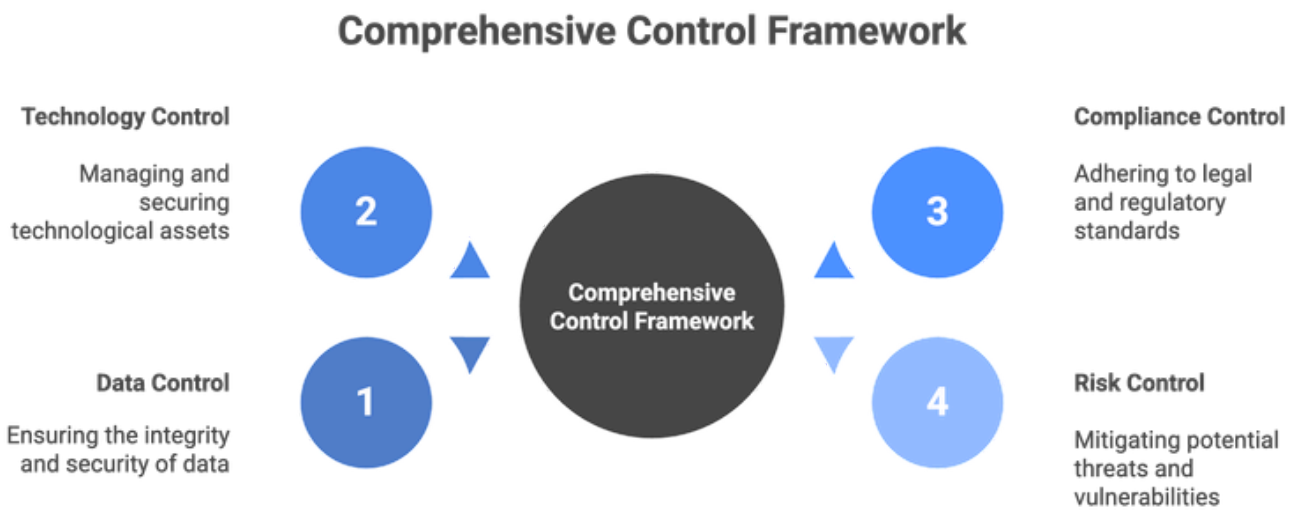
It includes:

1. Control over data
Where data is stored, processed, moved, and who has the legal right to access it.

2. Control over technology stack
Cloud infrastructure, software, applications, AI models, and vendor ecosystems.

3. Control over compliance and governance
The ability to independently meet regulatory requirements and prove compliance.

4. Control over digital risk
Avoiding exposure to foreign laws, surveillance, or unintentional data sharing.
Digital sovereignty is not just a legal requirement — it is a strategic necessity for operational continuity, cyber resilience, and long-term competitiveness.



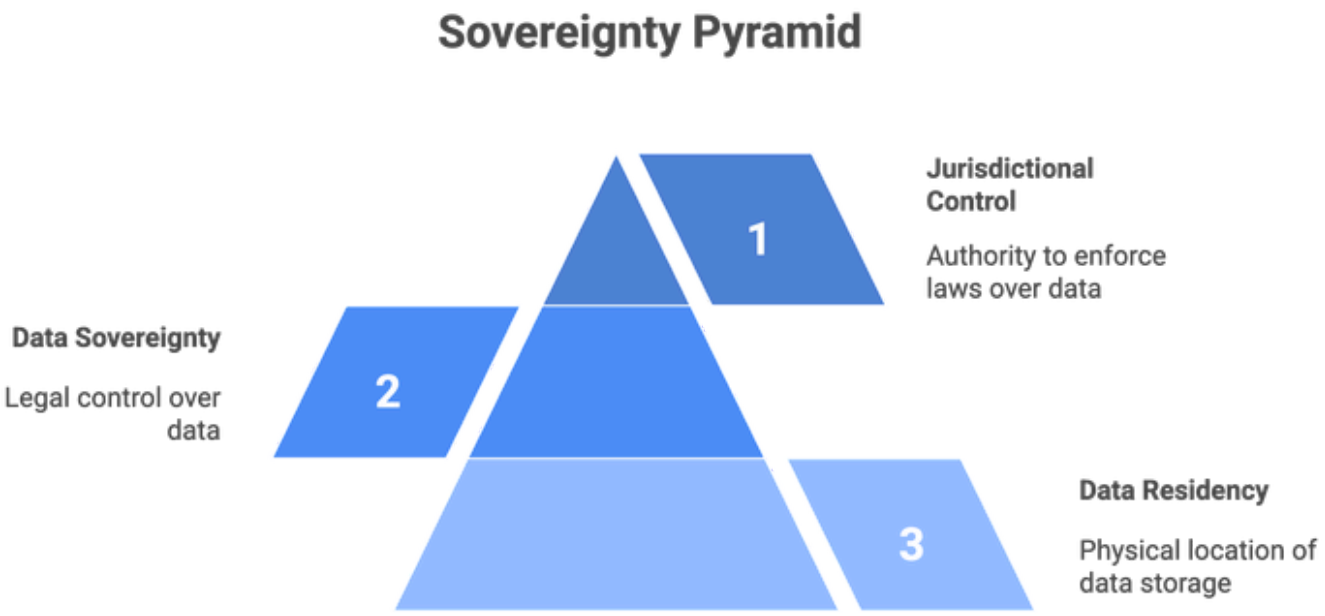
Residency vs Sovereignty vs Jurisdiction

Three Layers You Must Control

1. Data Residency
➤ Where your data is physically stored.

2. Data Sovereignty
➤ Which laws govern your data.

3. Jurisdictional Control
➤ Who can legally compel access to your data.

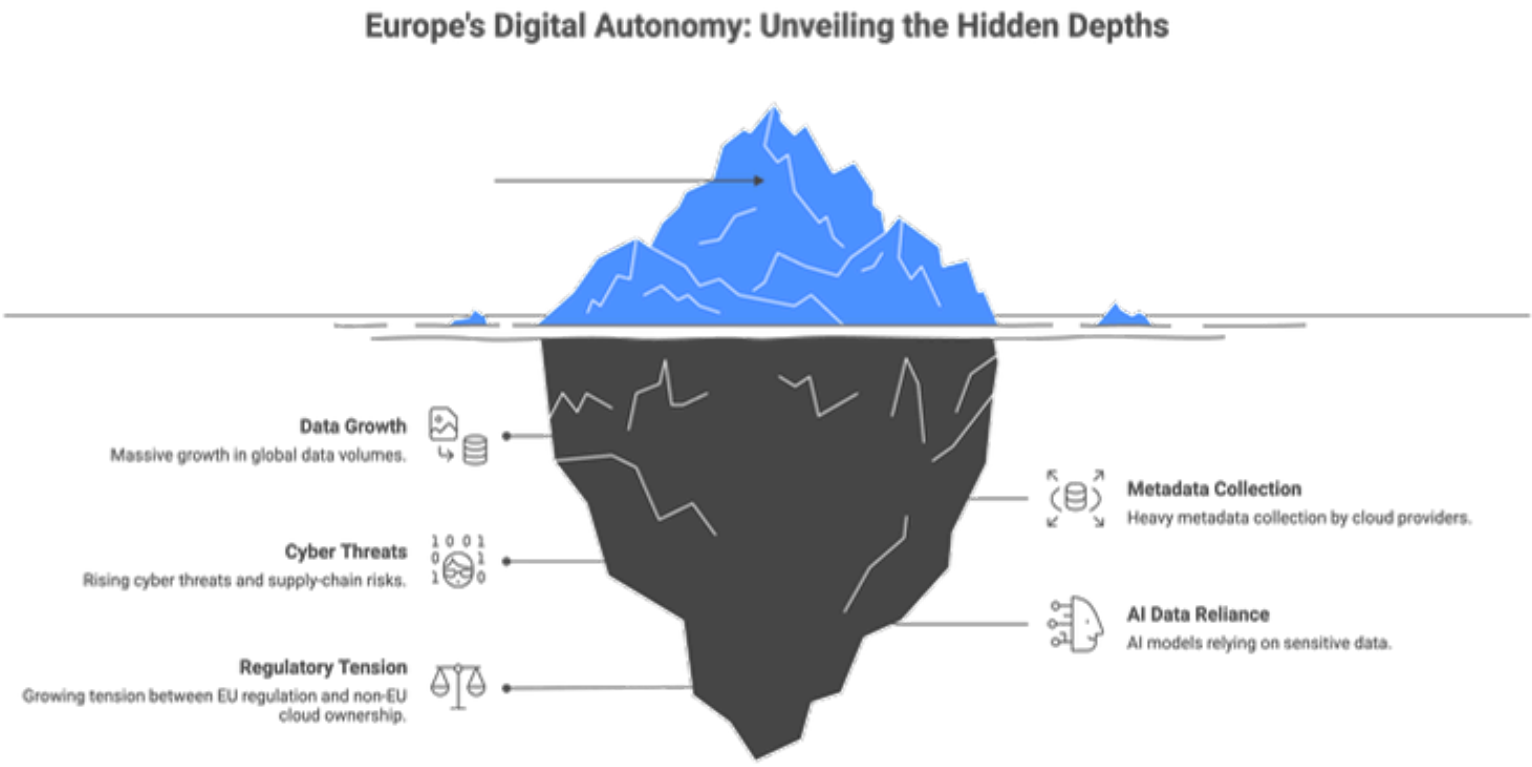


Why It Matters Now

Europe faces a turning point:

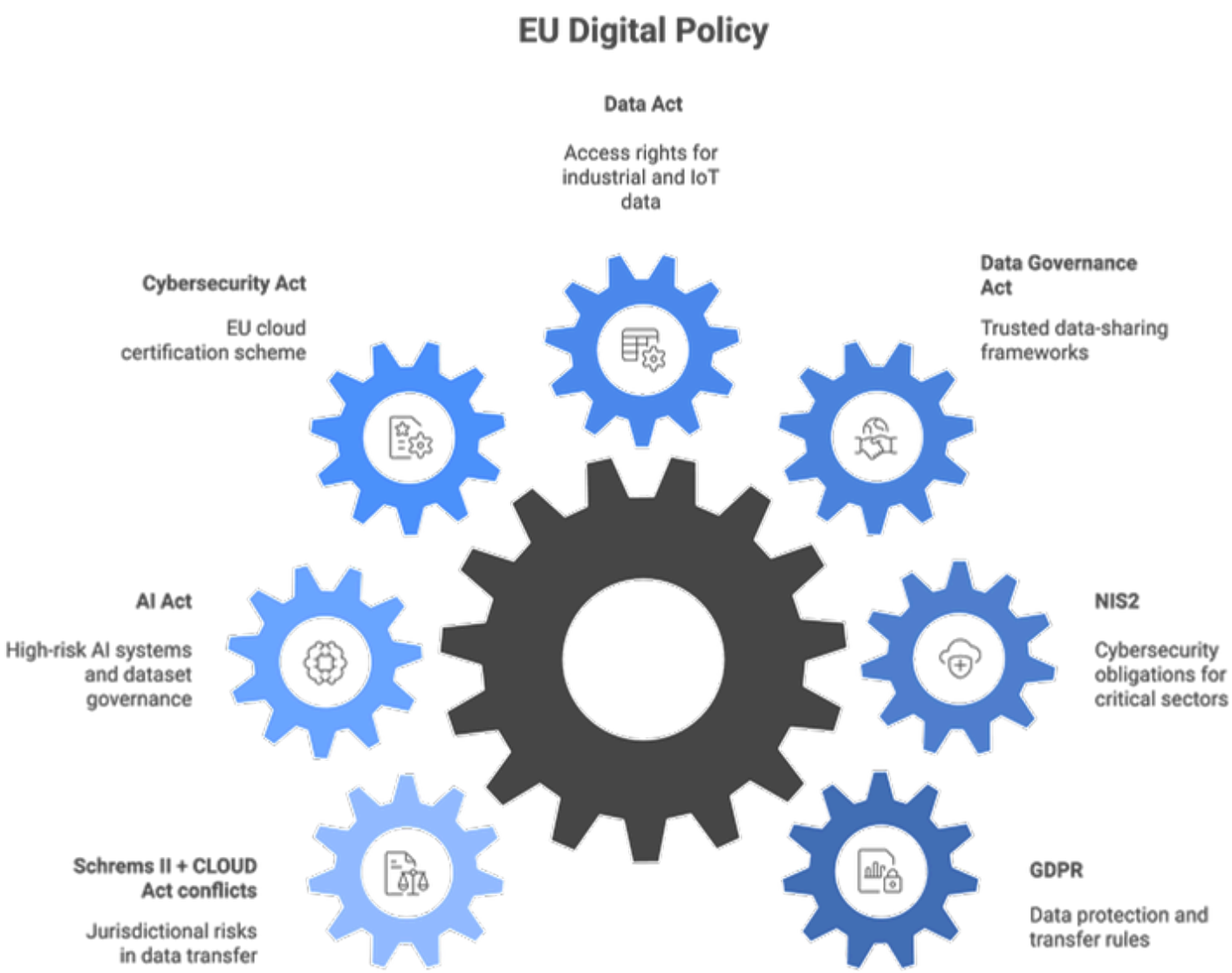
- Massive growth in global data volumes
- Heavy metadata collection by cloud providers
- Rising cyber threats and supply-chain risks
- AI models relying on sensitive data
- Growing tension between EU regulation and non-EU cloud ownership

Organizations must ensure digital autonomy to stay secure, compliant, and competitive.

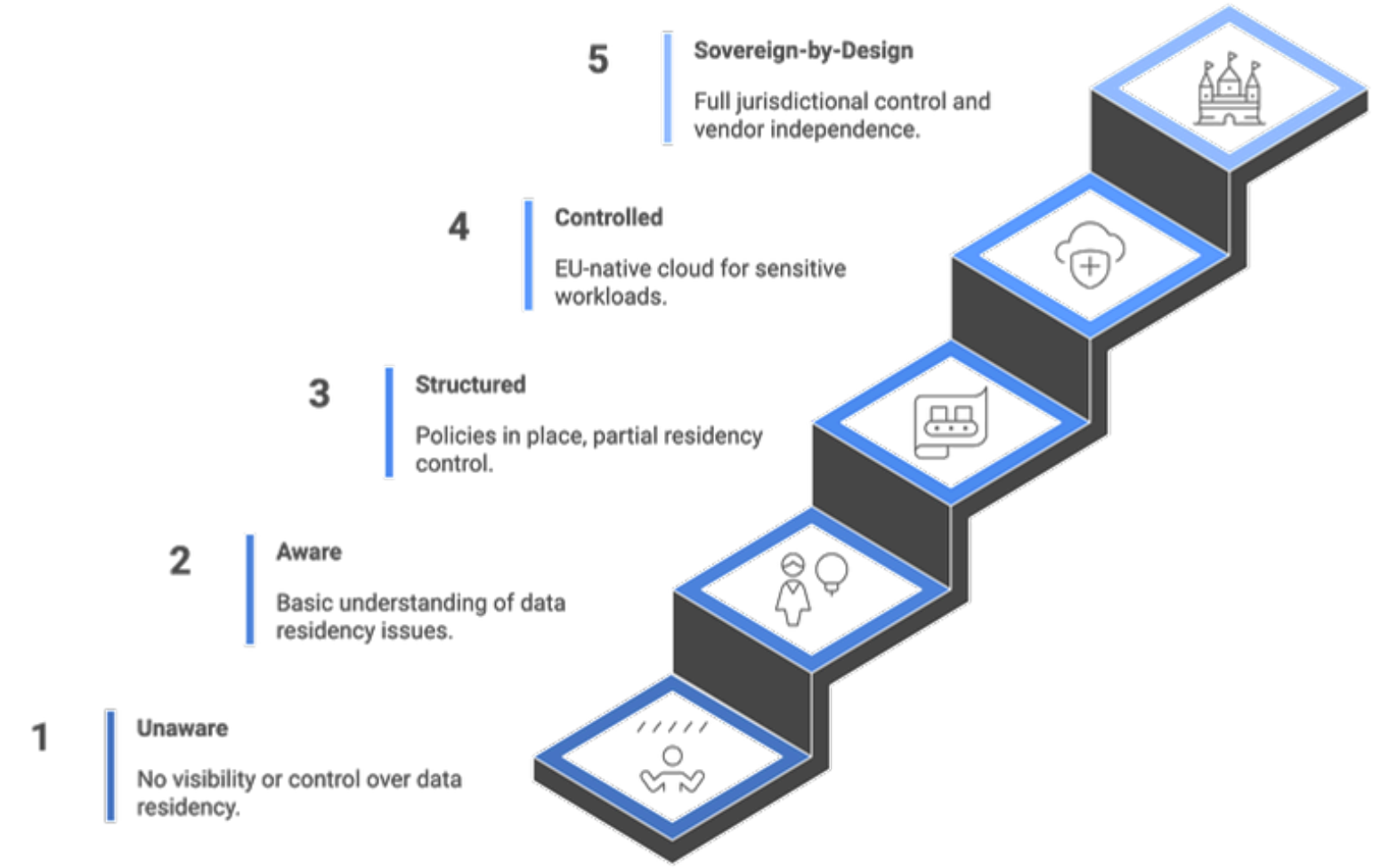


Key EU Regulations Shaping Your Cloud Strategy

- **GDPR** – Data protection & transfer rules
- **NIS2** – Cybersecurity obligations for critical sectors
- **Data Governance Act** – Trusted data-sharing frameworks
- **Data Act** – Access rights for industrial & IoT data
- **Cybersecurity Act** – EU cloud certification scheme
- **AI Act** – High-risk AI systems, dataset governance
- **Schrems II + CLOUD Act conflicts** – Jurisdictional risks



Digital Sovereignty Maturity Model



Digital Sovereignty Self-Assessment

Rate each question: 0 = No, 1 = Partially, 2 = Yes

A. Governance

- ☐ Do we know where all data is stored?
- ☐ Have we classified our data?
- ☐ Do we control metadata exposure?

B. Residency & Jurisdiction

- ☐ Are sensitive workloads stored exclusively in the EU?
- ☐ Can foreign laws apply to our data?
- ☐ Is our cloud provider EU-based?

C. Compliance & Monitoring

- ☐ Do we monitor compliance continuously?
- ☐ Are logs stored in the EU?
- ☐ Do we assess cross-border flows?

D. Cloud Architecture

- ☐ Do we classify workloads for sovereign deployment?
- ☐ Are backups jurisdiction-controlled?
- ☐ Do we isolate high-risk workloads?

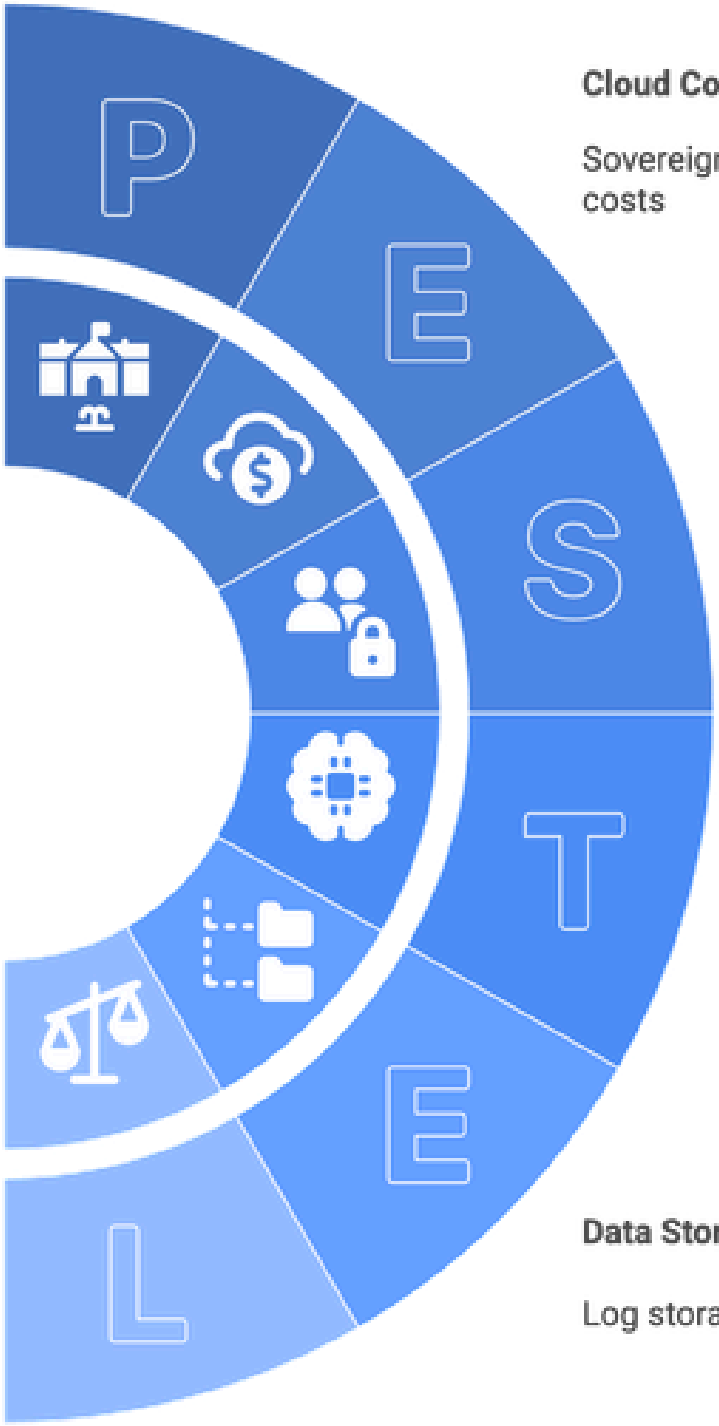
E. AI & Model Governance

- ☐ Do we store inference logs in the EU?
- ☐ Do vendors use our data for model training?
- ☐ Do we control model checkpoints?

Digital Sovereignty Self-Assessment

Data Residency

EU data storage



Cloud Costs

Sovereign deployment costs

Data Privacy

Metadata exposure control

AI Governance

Model checkpoint control

Data Storage

Log storage in the EU

Compliance

Continuous compliance monitoring

Sovereignty-by-Design Roadmap

1. Assess & Map
Identify data types, flows, and dependencies.

2. Govern & Steer
Define policies, ownership, and compliance frameworks.

3. Plan & Design
Architect sovereign-friendly cloud infrastructure.

4. Transform & Implement
Migrate workloads; enforce encryption and zero trust.

5. Run & Manage
Continuously monitor compliance and jurisdictional risk.

Sector-Specific Sovereignty Requirements

- **Public Sector**

Must retain strict jurisdictional control.

- **Banking & Finance**

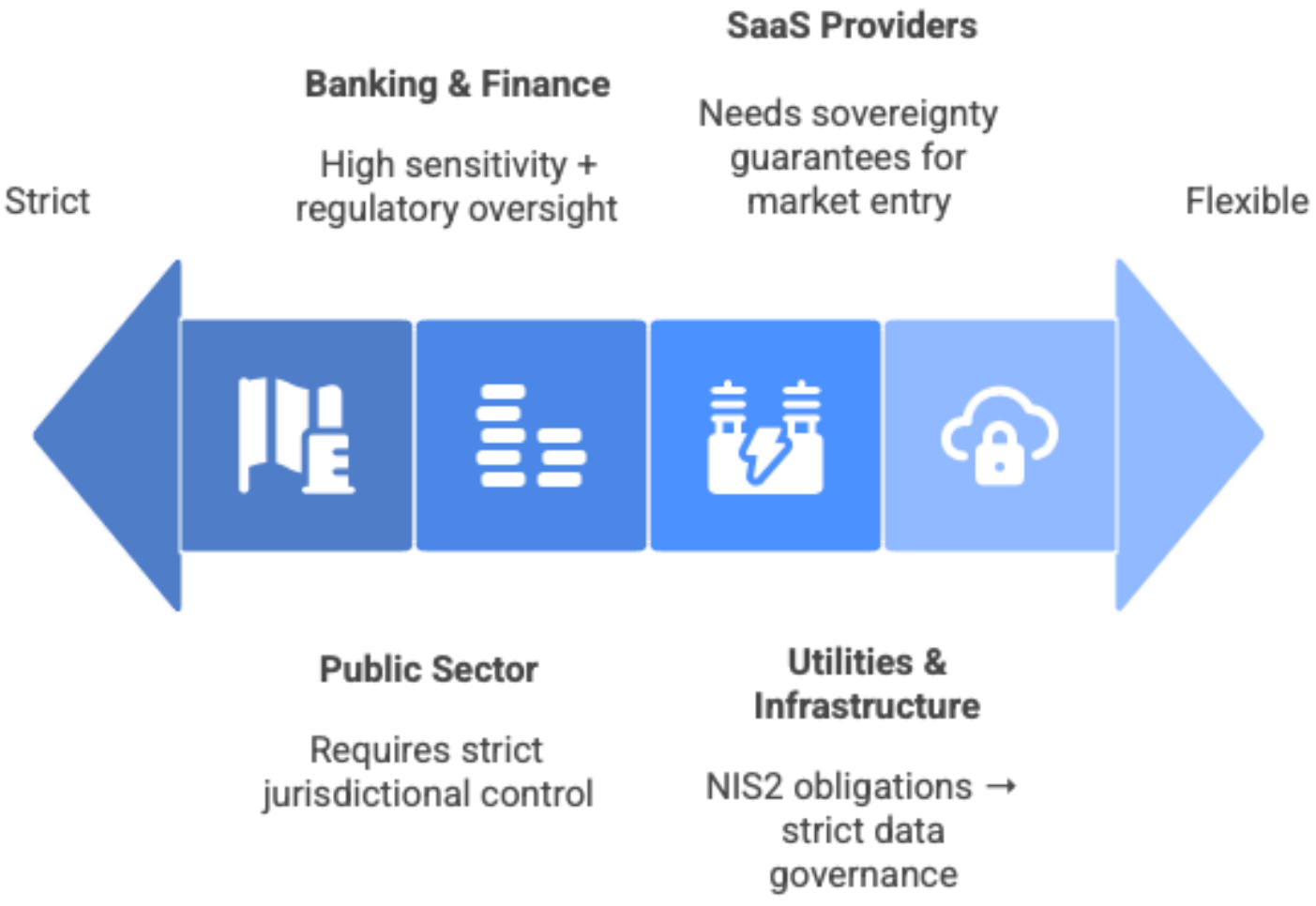
High sensitivity + regulatory oversight.

- **Utilities & Critical Infrastructure**

NIS2 obligations → strict data governance.

- **SaaS Providers**

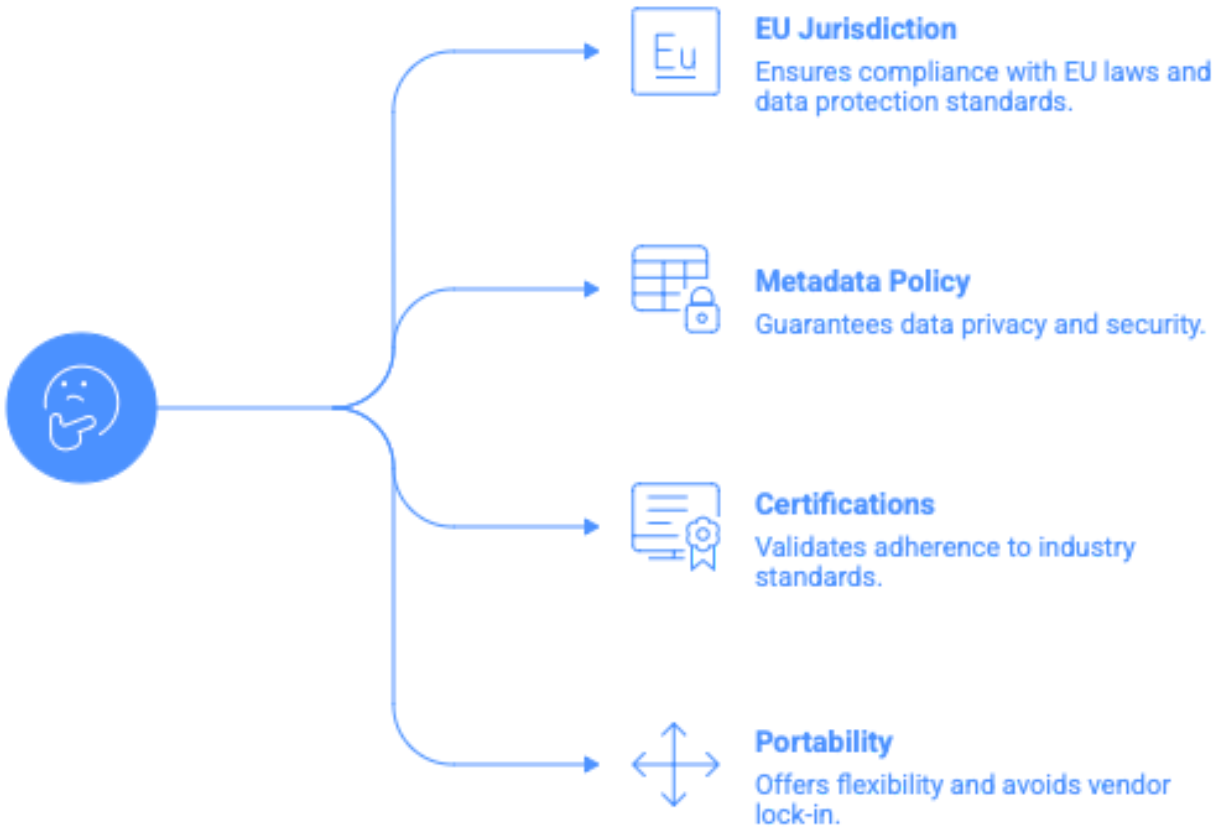
Need sovereignty guarantees to enter regulated markets.



How to Evaluate EU-Native Cloud Providers

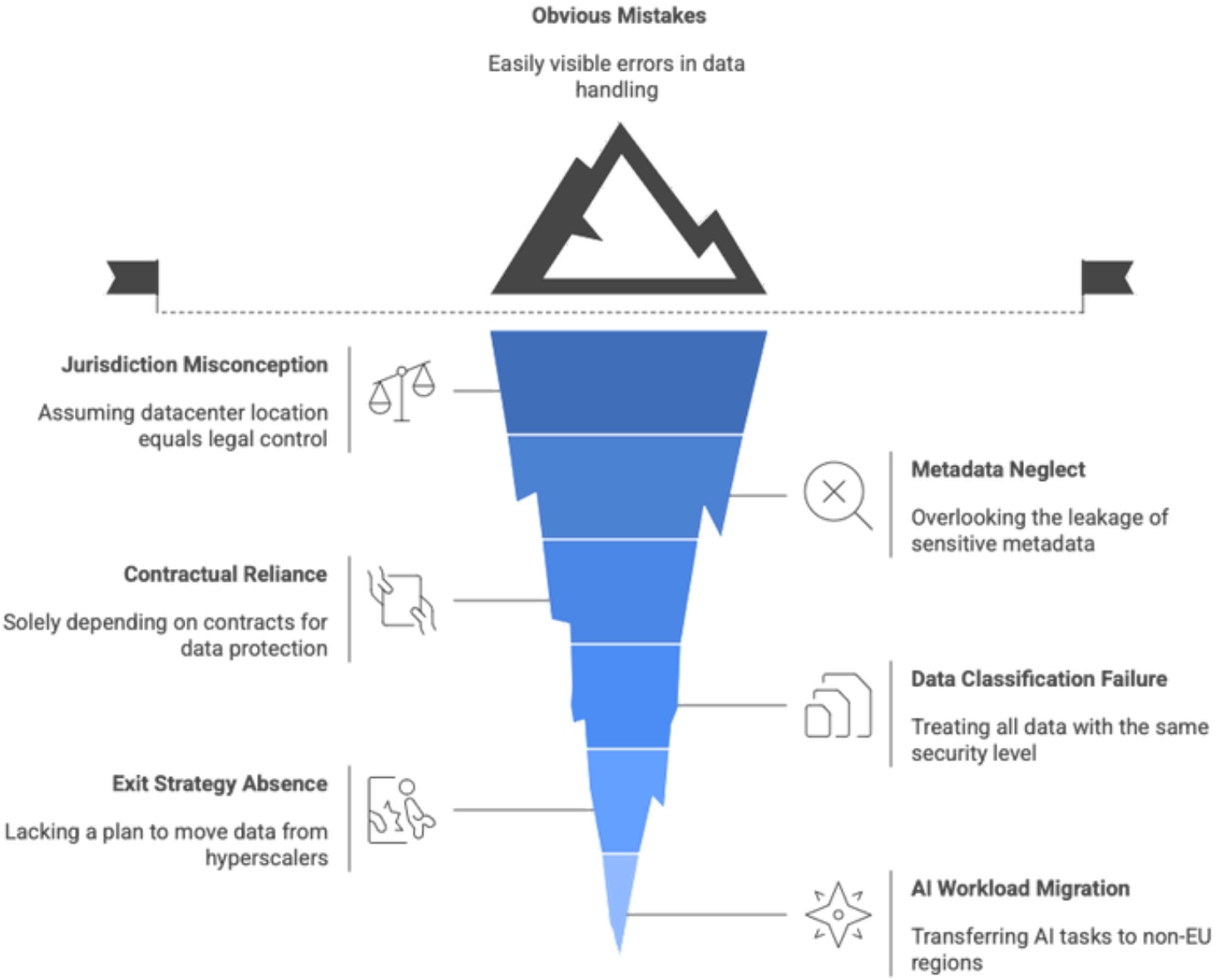
Choose providers that offer:

- EU ownership & headquarters
- No exposure to foreign jurisdiction
- Clear metadata governance
- EU-only operational staff
- Certified security frameworks
- Sovereign AI capabilities
- Vendor exit strategy
- Cost transparency



Avoid These Sovereignty Mistakes

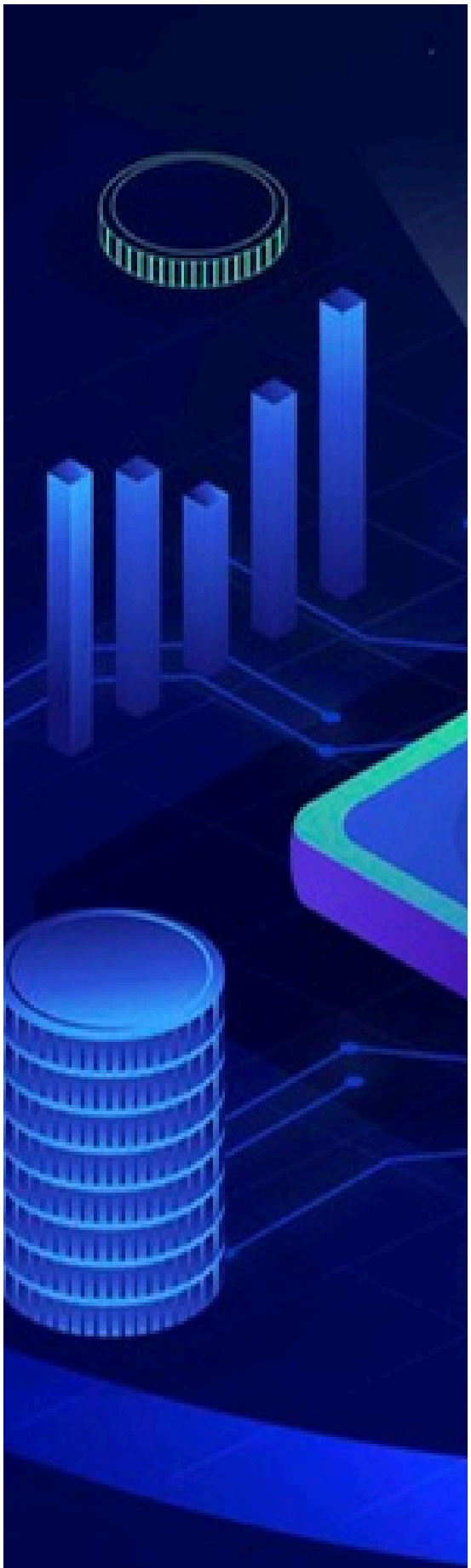
- Assuming EU datacenter = EU jurisdiction
- Ignoring metadata leakage
- Relying only on contractual clauses
- Classifying no data or all data the same
- No exit strategy from non-EU hyperscalers
- Moving AI workloads into non-EU regions



Glossary

- Digital Sovereignty – control digital assets independently
- Data Sovereignty – data governed by local laws
- Residency – physical data location
- Jurisdiction – legal power over data
- Zero Trust – no implicit trust model
- Sovereign Cloud – cloud aligned to local jurisdiction
- Metadata – descriptive operational information
- Portability – ability to migrate data freely

Need help assessing your sovereignty posture or evaluating EU-native cloud providers?



Use this assessment and roadmap to strengthen your strategy and build cloud infrastructure that protects your organization today.

Book a Digital Sovereignty Audit or Strategy Session now

Get in touch on the website or mail to: info@gartsolutions.com

gart.

Contributors

Fedir Kompaniiets

Co-Founder at Gart Solutions, DevOps and Cloud Solutions Consultant

Roman Burdiuzha

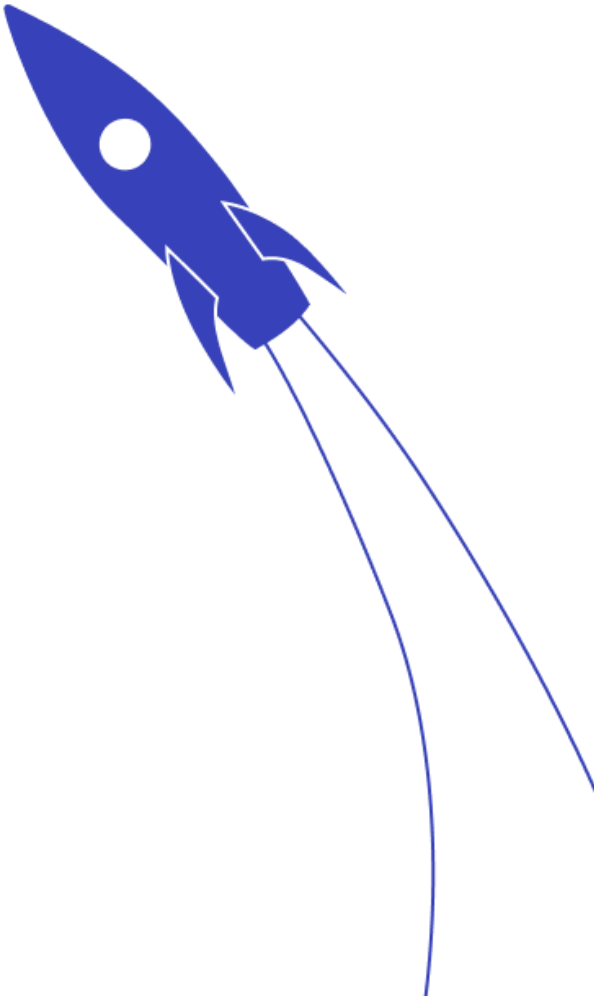
Cloud Architect, Co-Founder and CTO at Gart Solutions

gart.

Get in touch with us!

Gart Solutions is a Cloud and Devops services agency that provides businesses with infrastructure setup, automatization, cloud migration, cloud native development, CI/CD, and more.

We work to solve your tech challenges on time and budget and provide infrastructure with the endurance it needs
to let you focus on what matters the most – growing business.



gartsolutions.com

info@gartsolutions.com