emma

WHITE PAPER

CLOUD STRATEGY · 2026

The European CIO Guide to Building a Sovereignty-Compliant Cloud Strategy

How leading organisations balance compliance, innovation, and cost across sovereign environments — without choosing between the regulator and the product roadmap.

Alexey Romanov
Head of Engineering

CONTENTS

What's Inside

CHAPTER 01 · EXECUTIVE SUMMARY

The Sovereignty Dilemma

> **Data residency is not operational sovereignty. An EU-flagged region controlled by a non-EU corporate parent, subject to extraterritorial law, with no demonstrated exit capability, is not a sovereign posture.**

European organisations face a sovereignty dilemma that cannot be resolved with a single data locality decision. DORA, NIS2, and GDPR enforcement are tightening. Regulators are moving from guidance to audits. The most commonly proposed solutions — hyperscaler sovereign SKUs, migration to a single EU provider, or parallel cloud silos — create new problems without solving the underlying one.

What leading European CIOs are discovering is that operational sovereignty requires a governance layer that sits above and across providers — not inside any one of them. This means independently governed multi-provider architecture where workloads are placed by classification, policies are enforced at deployment time, and exit capability is built in by design.

CHAPTER 02 · THE SOVEREIGN CLOUD IMPERATIVE

Four Themes Driving Board-Level Urgency

Concentration Risk

DORA Article 29 requires financial entities to avoid undue dependence on single ICT providers. Most European enterprises are approaching this threshold. Regulators are beginning to define it numerically.

Extraterritorial Exposure

AWS, Azure, and GCP are US corporations subject to the CLOUD Act. Selecting an "EU region" does not change the corporate parent's legal obligations. EU-resident data in EU data centres remains compellable under US law.

Exit Planning as a Real Test

DORA Article 28(8) requires operational exit plans. Regulators are requesting evidence of tested procedures. Most organisations discover their plan is theoretical under scrutiny.

Hidden Cost of Sovereign SKUs

Hyperscaler sovereign offerings carry up to a 30% price premium over standard pricing. They restrict access to the latest AI and ML services not yet cleared for the sovereign tier. And they do not eliminate CLOUD Act exposure or resolve concentration risk findings.

CHAPTER 03 · THREE FLAWED APPROACHES

Why Each Conventional Response Fails

Most organisations confronting the sovereignty imperative consider three paths. Each has real advantages. Each also has structural failure modes that are frequently underestimated until a regulator or an incident exposes them.

APPROACH 01

Stay on Hyperscalers and Manage the Risk

The argument is straightforward. Hyperscalers offer advanced capabilities, global reach, AI and ML services, and a mature ecosystem. The problem is that regulators disagree. DORA audit findings can flag two issues: concentration risk and insufficient exit capability. Contractual portability clauses do not constitute a demonstrated exit plan. CLOUD Act exposure, even in EU regions, is increasingly documented as residual risk by DPOs and legal counsel. Regulatory requirements will continue to tighten, and an architecture designed to satisfy today's enforcement posture may need to be restructured within 24 months.

APPROACH 02

Migrate to a Single EU Provider

The appeal is clean: eliminate extraterritorial exposure by moving to a provider incorporated and operated under EU law. IONOS, OVHcloud, and Scaleway offer genuine EU sovereignty and competitive pricing. The structural failure mode is the service catalogue gap. EU-native providers cannot match hyperscaler depth in managed AI and ML services. Organisations that migrate entirely report a significant innovation penalty. There is also a second-order risk: new lock-in. Moving from one provider dependency to another does not solve the structural problem.

APPROACH 03

Run Parallel Cloud Silos

The most common compromise: maintain hyperscaler infrastructure for innovation workloads while standing up EU-native infrastructure for regulated workloads. In practice, both environments are usually kept operationally separate. This creates significant complexity. Platform teams must context-switch between environments. Security policies must be maintained separately. Cost visibility fragments. Organisations that have run this model report that compliance overhead of the dual-silo approach often exceeds the cost of the compute itself.

> **None of these approaches resolves the sovereignty dilemma. Each trades one set of problems for another. The architecture that actually resolves it requires a unified governance layer that sits above all providers — independent of every one of them.**

CHAPTER 04 · THE MULTI-PROVIDER GOVERNANCE MODEL

How the Architecture Works

The architecture that resolves the sovereignty dilemma is a governed multi-provider model with an independent operational control layer sitting above all providers. The key word is independent. The governance layer must not be provided by or dependent on any of the cloud providers it governs.

Workload Classification

Classification drives placement. A typical framework has four tiers: Critical-Regulated (EU-native, full jurisdictional control), Sensitive (strongly preferred EU-native), Standard (hyperscaler acceptable with governance enforcement), and Innovation (hyperscaler optimal for AI and ML). Not all workloads require the same sovereignty posture, so treating them uniformly creates unnecessary cost constraints or compliance gaps.

Private Cross-Provider Connectivity

Cross-provider connectivity is managed through a private backbone, not the public internet. Predictable, low-latency connectivity between sovereign environments and governed hyperscalers makes the architecture viable for latency-sensitive workloads including real-time fraud detection and transaction processing.

Policy Enforcement at Deploy Time

Policies are enforced before the workload is provisioned instead of being verified afterward. When a developer runs a deployment, the governance layer checks the classification, validates the target environment against the applicable policy, and either approves or blocks. Drift prevention catches manual changes that bypass the automated workflow.

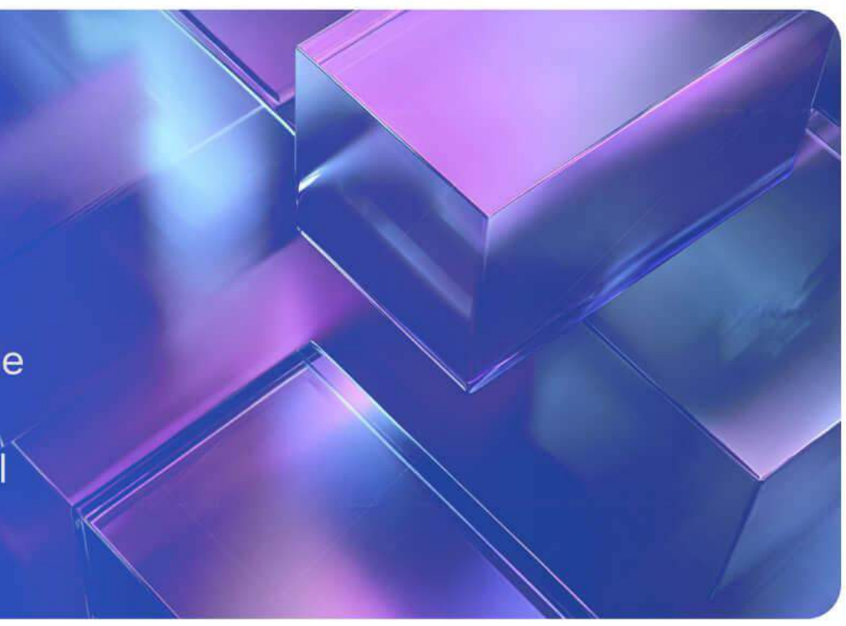
Continuous Audit Evidence

Rather than assembling compliance documentation at audit time, the governance layer maintains immutable logs of every deployment decision, every policy check, and every data flow. Regulators receive documentation reflecting the real state of the infrastructure instead of a point-in-time snapshot assembled by hand.

TRUE WORKLOAD MOBILITY

Why This Answers the DORA Exit Requirement

Because workloads are portable by design, exit capability is demonstrable. You can show a regulator the workload classification, the provider selection logic, and the deployment automation that would execute a migration. That is different evidence than a mere contractual clause stating you have the right to migrate.



Up to 30%

Price premium on hyperscaler sovereign SKUs vs standard pricing

Up to 50%

EU-native provider pricing below hyperscaler EU-region rates

20–30%

Typical reduction in cloud spend for the migrated workload set

CHAPTER 05 · IMPLEMENTATION FRAMEWORK

Phased Implementation Approach

WEEKS 1–2

Map the Current State

PHASE 1 | Audit

Catalog every workload and its current provider placement, identify data classification and regulatory sensitivity, and trace the supplier chain including subprocessors. Organisations frequently discover that the actual dependency footprint is larger than the contract list suggests — CDN dependencies, logging services, and identity providers may all route through non-EU infrastructure.

WEEKS 3-4

Target Architecture and Policy Set

PHASE 2 | Design

Establish the target architecture and provider selection for each tier. Policy design translates regulatory requirements into machine-readable rules covering data residency, access controls, encryption, and audit logging. Policy rules should be version-controlled and reviewed by internal audit and legal counsel before deployment.

WEEKS 5-8

Progressive Rollout

PHASE 3 | Deploy

Progressive rollout begins with low-risk workloads — development environments, non-regulated analytics, internal tooling. Every workload migrated should use the same automation and runbooks as a real exit scenario. The first 20 migrations are also the first 20 rehearsals of the exit procedure.

CHAPTER 06 · FINANCIAL CASE

The Economics of Multi-Provider Governance

Hyperscaler sovereign SKUs often carry a price premium. EU-native providers can price up to 50% below hyperscaler standard rates. An organisation that moves regulated workloads from hyperscaler sovereign tiers to EU-native providers while maintaining hyperscaler access for innovation can easily see a 20–30% reduction in total cloud spend for the migrated workload set. The compliance overhead reduction from automated evidence generation, roughly 40–60 hours of monthly manual work, is an additional, substantial operational benefit.

SMART SOVEREIGNTY

Innovation Preservation

An organisation that migrates entirely to EU-native providers sacrifices hyperscaler AI and ML services without EU-native equivalents. Governed multi-provider architecture preserves access to hyperscaler innovation while enforcing sovereignty requirements where they apply. This is the architecture that satisfies both the regulator and the product roadmap.

CHAPTER 07 · ORGANISATIONAL ALIGNMENT

Stakeholder Frames

Stakeholder alignment is the most frequently underestimated implementation challenge. The technical architecture is tractable. Getting CIO, CISO, CFO, and DPO aligned on a shared frame is harder — and each frame is valid on its own terms.

CIO / CTO

Multi-provider governance is the architecture that allows compliance with current and anticipated regulatory requirements without foregoing innovation capability. It is an infrastructure strategy decision, not a compliance project managed by the security team.

CISO

The multi-provider architecture reduces concentration risk, enforces consistent security policy across all environments, and maintains SOC operations under EU jurisdiction with continuous compliance monitoring and immutable audit evidence.

CFO

Migration of regulated workloads to EU-native providers reduces the premium paid for hyperscaler sovereign SKUs. Automated evidence generation reduces compliance staffing overhead. Documented exit capability reduces regulatory fine risk.

DPO

EU-incorporated governance layer and EU-native placement for regulated workloads eliminates the extraterritorial law exposure that an EU-region hyperscaler deployment does not resolve. Data processor agreements are with EU-incorporated entities governed by EU law.

CHAPTER 08 · TYPICAL USE CASES

Illustrative Scenarios Across Sectors

FINANCIAL SERVICES

DORA Compliance with Continued AI Innovation

Consider a top-10 European retail bank with EUR 150B AUM that receives an internal audit finding of material concentration risk on a single hyperscaler. The board mandates demonstrable exit capability within 12 months; the CTO requires zero impact on AI development velocity. In this scenario, regulated data and transaction systems migrate to EU-native providers under emma governance, while AI and ML infrastructure remains on the hyperscaler under emma governance with enforced EU-region placement. A private backbone maintains sub-8ms latency for real-time applications.

~100%	~40%	~25%	0	2M+ €
DORA compliance via live exit simulation	Compliance overhead reduction	Lower cloud spend	AI velocity impact	Avoided duplication costs

HEALTHCARE RESEARCH

GDPR-Aligned Research at Scale

A European genomics research organisation processing GDPR Article 9 special category data could use emma to prove research data never transits non-EU infrastructure, while retaining access to large-scale GPU compute. Primary data remains on EU-native infrastructure with emma-enforced residency, while model training with anonymised data sets runs on hyperscaler GPU with policies ensuring no raw genomic data leaves EU-resident storage.

- GDPR compliance with immutable logs
- Research velocity maintained

MANUFACTURING

IP Protection with Supply Chain Integration

A mid-market European manufacturer operating across six EU countries could connect production systems and supply chain partners while protecting proprietary process data and meeting NIS2 requirements. Operational technology would run on EU-native private cloud and supply chain integration workloads on a governed hyperscaler, with data classification policies enforced automatically by emma.

- NIS2 compliance achieved
- IP protection automated

CHAPTER 09 · CONCLUSION

Sovereignty as Competitive Advantage

European organisations that achieve genuine operational sovereignty gain a durable competitive advantage. The regulatory moat that DORA, NIS2, and GDPR create is not a burden for organisations that have built the right architecture. It is a barrier to entry for non-EU competitors and a trust signal for EU customers, partners, and regulators.

The organisations that will lead in the European market over the next decade are those that build multi-provider access and governance into their infrastructure strategy now. They will be the ones with demonstrated exit capability, automated compliance evidence, and preserved access to the AI innovation services that will define competitive advantage.

The architecture exists. The providers are ready. The governance tooling is operational. The remaining variable is organisational will.

> “Make cloud work for you.
>
> European organisations need an architecture that satisfies the regulator and the product roadmap simultaneously. Governed multi-provider infrastructure is that architecture — and the evidence is now in from organisations that have implemented it. ”

Alexey Romanov
Head of Engineering

References

- EU Cloud Sovereignty Framework v1.2.1
- Digital Operational Resilience Act (DORA) — Regulation (EU) 2022/2554
- NIS2 Directive — Directive (EU) 2022/2555
- GDPR — Regulation (EU) 2016/679
- ENISA Cloud Cybersecurity Market Analysis
- US CLOUD Act — Clarifying Lawful Overseas Use of Data Act (2018)
- SecNumCloud — ANSSI Cloud Security Certification Framework
- C5 — Cloud Computing Compliance Controls Catalog (BSI)
- ISO/IEC 27001:2022 — Information Security Management

TAKE THE NEXT STEP

Ready to Strengthen Your Sovereignty Posture?

See how emma gives your team unified control across every cloud provider — with governance that holds everywhere by design. Book a 30-minute sovereignty review with an emma Solutions Architect.

30 min

focused review

100%

cloud-agnostic

1 call

clear next steps

BOOK A SOVEREIGNTY REVIEW →

No commitment required · Free 30-min session

About emma

The cloud operations platform for distributed sovereign infrastructure

emma is built for organisations running distributed workloads across hybrid and multi-cloud environments — where operational complexity, unpredictable costs, and strict regulations get in the way of building.

It provides a single, policy-driven operating layer that spans hyperscalers, regional European cloud providers, AI-optimized infrastructure, and on-premises environments. From one dashboard, engineering, platform, and finance teams can deploy workloads, enforce compliance policies, and view and govern their entire infrastructure footprint. Sovereignty and compliance are built in through proactive guardrails, not bolted on.

With a vendor-neutral architecture, emma ensures organisations can choose the right infrastructure for cost, performance, and regulatory requirements — without lock-in or operational trade-offs.

Data Residency & Jurisdictional Control

Data stays within defined geographic and legal boundaries, which are enforced at the infrastructure layer across every environment rather than relying on policy documents.

Policy-Driven Workload Placement

Provider eligibility and sovereign constraints are maintained as infrastructure guardrails at deployment time, ensuring workloads run only in approved environments across providers.

Network Boundary Control

Cross-cloud data moves over emma's private networking backbone instead of the public internet. This reduces cross-border public routing exposure within and between jurisdictions.

Encryption & Key Sovereignty

Encryption and key management policies are also enforced at deployment time. Organisations retain control over who holds the keys, regardless of where workloads run.

Provider Portability & Exit Readiness

Tested migration paths across providers reduce concentration risk and meet regulatory exit capability requirements before they become urgent.

Continuous Governance & Compliance Evidence

Workloads are continuously evaluated against policies that align with GDPR, NIS2 and DORA. Audit-ready logs mean compliance evidence is generated automatically.

2021
Founded & HQ in Luxembourg

15+
Cloud providers supported

~90
Cloud engineers at your service

NO
US Cloud Act applicability

CERTIFICATIONS & FRAMEWORKS

emma operates under internationally recognized security and compliance frameworks, including ISO-certified security management and SOC 2 Type II audited controls, with data protection aligned to GDPR and resilience aligned with NIS2 and DORA.

NEXT STEPS

Contact us

emma.ms

info@emma.ms

19-21 Rte d'Arlon, 8009 Strassen, Luxembourg

emma | Make Cloud Work for You