

DOSOBÉ.

AI Governance & Digital Sovereignty

Operating Models, Frameworks, and Strategic Imperatives

DOSOBÉ Research White Paper — June 2026

Classification: Public

Table of Contents

1. Executive Summary

2. AI Governance Operating Models

3. Cloud Sovereignty for Agentic AI

4. Europe Digital Sovereignty

1. Executive Summary

As autonomous AI systems become integral to enterprise operations, the governance frameworks that oversee them must evolve. Traditional IT governance, designed for deterministic systems with clear human accountability, is insufficient for agentic AI where decisions are autonomous, behaviour is emergent, and accountability is distributed across multiple actors.

Digital sovereignty adds another dimension: the ability of organisations and nations to control their technological infrastructure and data. In the age of agentic AI, sovereignty extends to control over autonomous decision-making systems that increasingly mediate economic and social activity.

This white paper examines the intersection of AI governance and digital sovereignty, providing frameworks for organisations navigating both dimensions.

2. AI Governance Operating Models

Effective AI governance requires an operating model that addresses five dimensions: risk classification, oversight structure, accountability assignment, monitoring and reporting, and remediation processes.

2.1 Centralised vs Distributed Models

Centralised governance establishes a Centre of Excellence that sets policies, reviews deployments, and monitors compliance across the organisation. Distributed governance delegates these responsibilities to business units with coordination through standards and audits.

2.2 The DOSOBÉ Three-Line Model

First Line: AI system owners and developers are responsible for building compliant systems and operating within defined parameters.

Second Line: An AI governance function sets policies, provides guidance, and monitors compliance across all deployments.

Third Line: Internal audit provides independent assurance that governance processes are operating effectively.

Governance is not a constraint on innovation. It is the foundation that enables responsible innovation at scale.

3. Cloud Sovereignty for Agentic AI

Cloud sovereignty is the ability of an organisation to maintain control over its data and operations when using cloud infrastructure. For agentic AI, cloud sovereignty takes on additional significance because autonomous agents make decisions that may have legal, regulatory, and ethical implications.

3.1 Sovereignty Requirements for Agentic AI

- **Data Residency:** Guarantees that data remains within specified jurisdictions
- **Operational Control:** Ability to audit, intervene in, and override agent decisions
- **Regulatory Compliance:** Adherence to sector-specific regulations across jurisdictions
- **Vendor Independence:** Avoidance of lock-in to proprietary AI platforms

4. Europe Digital Sovereignty

Europe path to digital sovereignty is shaped by regulatory frameworks, infrastructure investments, and technological capabilities. The EU AI Act, Data Governance Act, and Digital Markets Act create a distinct regulatory environment.

4.1 The Regulatory Stack

The EU AI Act establishes risk-based classification for AI systems. The Data Governance Act creates frameworks for data sharing. The Digital Markets Act regulates gatekeeper platforms. The emerging AI Liability Directive addresses liability for autonomous system harm.

Key Insight

Organisations building for European standards from the start are better positioned for global deployment than those optimising for less regulated markets.

5. Multi-Agent Data Governance

Multi-agent AI systems introduce data governance challenges that traditional frameworks cannot address. Data moves between agents, is transformed by each agent, and informs autonomous decisions. Ownership, lineage, and quality assurance become runtime concerns.

5.1 Inter-Agent Data Lineage

Our framework tracks every data transformation through a provenance graph recording which agent modified the data, what transformation was applied, and under which policy.

5.2 Quality at Consumption

Consuming agents evaluate data quality based on provenance metadata, freshness, and consistency with expected distributions. Low quality triggers correction, rerouting, or escalation.

6. Strategic Recommendations

Priority	Action	Timeline
Critical	Establish AI governance operating model with clear three-line accountability	0-3 months
High	Audit cloud sovereignty posture for agentic AI workloads	3-6 months
Medium	Implement multi-agent data lineage tracking	6-9 months
Ongoing	Monitor regulatory developments in AI governance	Continuous