

How to design for data sovereignty

An enterprise checklist

Data sovereignty is no longer about where data sits. It is about whether organizations can control and prove how data is stored, accessed, and moved across distributed environments.

As cloud, third-party, and AI-driven data flows grow, risk often increases during transit, across the routes, intermediaries, and jurisdictions data passes through. Regulators and auditors also expect controls that are operational and verifiable, not just documented. For enterprises, this means treating sovereignty as a design requirement that reduces exposure without slowing performance or innovation.

Use the following checklist to design your network for data sovereignty.

An enterprise checklist

1.

Identify your AI ecosystem before designing for sovereignty

- List AI use cases and the data they depend on (training, inference, RAG, agents)
- Map data sources (internal apps, SaaS, partners, public sources)
- Map where data is stored, replicated and processed (cloud/on-prem/third party)
- Map key integrations between environments (cloud-to-cloud, cloud-to-DC, DC-to-SaaS)
- Confirm ownership for each system and dataset (business + technical)

2.

Align data criticality with risk tolerance

- Classify data by sensitivity and regulatory requirement (by jurisdiction if needed)
- Classify workloads by criticality (business impact of loss/compromise/outage)
- Define acceptable exposure “in transit” for each tier (where it can/can’t traverse)
- Set minimum controls per tier (encryption, access, logging, routing constraints)
- Document exceptions and approval path (so deviations are visible and governed)

3.

Design for provability

- Define what you must be able to evidence to auditors/regulators (routes, controls, responsibilities)
- Ensure you can describe how traffic enters/exits each provider network
- Reduce unnecessary intermediaries and third-party network hops
- Validate routing behavior for key flows (especially cross-border and third-party paths)
- Put in place monitoring/logging that supports ongoing assurance (not one-off checks)

4.

Scrutinize providers and their supply chains

- Confirm network provider ownership and operating entities (by region, where relevant)
- Identify which third parties the provider relies on (cloud, hardware, network partners)
- Clarify where services are delivered from and where management access may occur
- Review supplier controls for security, compliance and change management
- Require transparency and auditability clauses aligned to your sovereignty needs

5.

Strengthen protection around exposed environments

- Identify internet-adjacent and SaaS-connected environments (highest exposure)
- Review how connections are secured and controlled in transit
- Reduce exposure to third-party networks where possible (more direct connectivity)
- Validate redundancy/diversity for critical paths and test failover scenarios
- Confirm performance under disruption and how incidents are handled/escalated