Data Sovereignty

Balancing control and trust

Data sovereignty has moved from IT conversations to boardroom discussions. For organisations operating across European borders, the question is no longer if data sovereignty matters but securing the right balance of who has control of your data.

Scroll to learn more

It's About Control, Not Just Location

Data sovereignty is about your ability to make decisions around your data. Where it goes. Who can access it. How it's protected. When you can retrieve it. The moment those decisions move beyond your influence, you've lost sovereignty – regardless of where the data physically resides.

> Data residency = Where your data is stored
> Data sovereignty = Who controls it

The 4 Pillars Of Data Sovereignty

1 Data
What needs protecting and where flow?

2 Legal Jurisdiction
Which laws and regulations apply?

3 Operational Controls
Who can access your systems and under what circumstances?

4 Technical Controls
Can you enforce sovereignty through architecture and security?

The Control Paradox

Maximum control doesn't mean maximum security.
Pursuing absolute control creates its own vulnerabilities:

Capability Gaps
Can you defend against AI-driven threats 24/7?
Resource constraints
Do you have the expertise and investment needed?

Innovation Lag
Can you keep pace with evolving threats?
Single points of failure
What happens during staff turnover or budget cuts?

> Effective data sovereignty isn't about maximising control. It's about managing risk and maintaining the right controls.
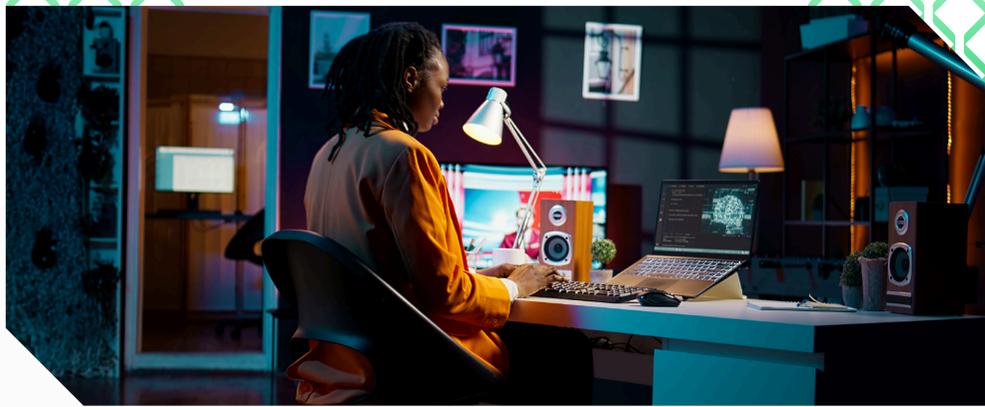
3 Forces Making Data Sovereignty Urgent Now

1 Regulatory Intensification
GDPR, NIS2, DORA, and the emerging AI Act mandate not just where data is stored, but who controls it and how it's processed.

RISK: Inability to demonstrate appropriate oversight creates compliance risk and potential penalties.

2 Geopolitical Uncertainty
Can you trust your infrastructure will remain available if geopolitical events restrict cross-border data flows?

RISK: Loss of competitive advantage as European governments and enterprises increasingly prioritise sovereign solutions.

3 Infrastructure Misalignment
Some providers prioritise operational efficiency over jurisdictional compliance. Terms can change unilaterally, and exit strategies are often prohibitively expensive.

RISK: Stakeholders need assurance you maintain control over sensitive data – vendor lock-in undermines that assurance.

Building Trust

The foundation of data sovereignty

When you engage vendors, you're partnering for enhanced capability. The key is choosing partners who enhance your control rather than diminish it. What builds trust?

Track Record
Years of protecting organisations like yours

Transparency
Clear data handling, comprehensive reporting, continuous auditability

Local Commitment
Physical presence, regulatory alignment, cultural understanding

Proven Compliance
Certifications that matter (ISO 27001, SOC 2, GDPR frameworks)

Exit Flexibility
Confidence you can retrieve data and migrate if needed

Start Your Data Sovereignty Journey

Veeam's experts can help you:

Our experts understand the balance between control and capability that European organisations must strike to maintain control while providing the protection, resilience, and compliance capabilities you need.

We'll determine which solutions are suitable for your organisation and demonstrate how Veeam can become a trusted partner in your data sovereignty journey.

- Offices in 20+ European cities
- 5,000+ partners worldwide
- Local data centres

LETS TALK