Digital sovereignty

Rebuilding our digital foundations

Over 80% of digital products in Europe depend on providers **beyond our jurisdiction**.[1] Hyperscalers like Google, Amazon, and Microsoft drive European innovation. But our reliance on them exposes us to geopolitical forces we can't control, including laws like the U.S. CLOUD Act, which allows American authorities to access data held by U.S.-based providers even if it's stored in Europe.

Concern over this dependency has been mounting, with recent events exposing the risks. At Amsterdam Trade Bank, sanctions cut off access to critical US cloud systems, freezing operations despite **the bank being solvent and Netherlands-regulated**.[2] The same year, the Dutch Justice Ministry warned government agencies against **using Microsoft for sensitive data**;[3] by 2025, parliament had passed motions urging reduced **reliance on U.S. providers**.[4] Denmark has gone even further, moving to phase out the use of Microsoft in government completely **in favour of open-source alternatives**.[5] AI raises the stakes even higher.

AI models require vast amounts of data, much of which is sensitive, and often processed on foreign-controlled cloud platforms. In response, European organisations are finding ways to localise sensitive data and diversify infrastructure without sacrificing innovation.

Just look at Belgium's Proximus, a partly state-owned telco vital to national infrastructure, which handles a wide range of data and applications. For highly sensitive workloads, it relies on EU-based or locally managed cloud infrastructure. But, for everyday workloads, it leverages global hyperscalers, demonstrating that **sovereignty and openness can coexist**.[6]

But every sovereignty challenge is unique. A bank's critical systems differ from a telco's infrastructure, and a government agency faces different threats than a manufacturer. The question isn't whether to act, it's where to start and how fast to move. We share how you can navigate them with confidence.

> "Innovation requires trust: trust in your data, your systems, your ability to make decisions. That's what digital sovereignty gives you, and that's what we help our clients achieve."

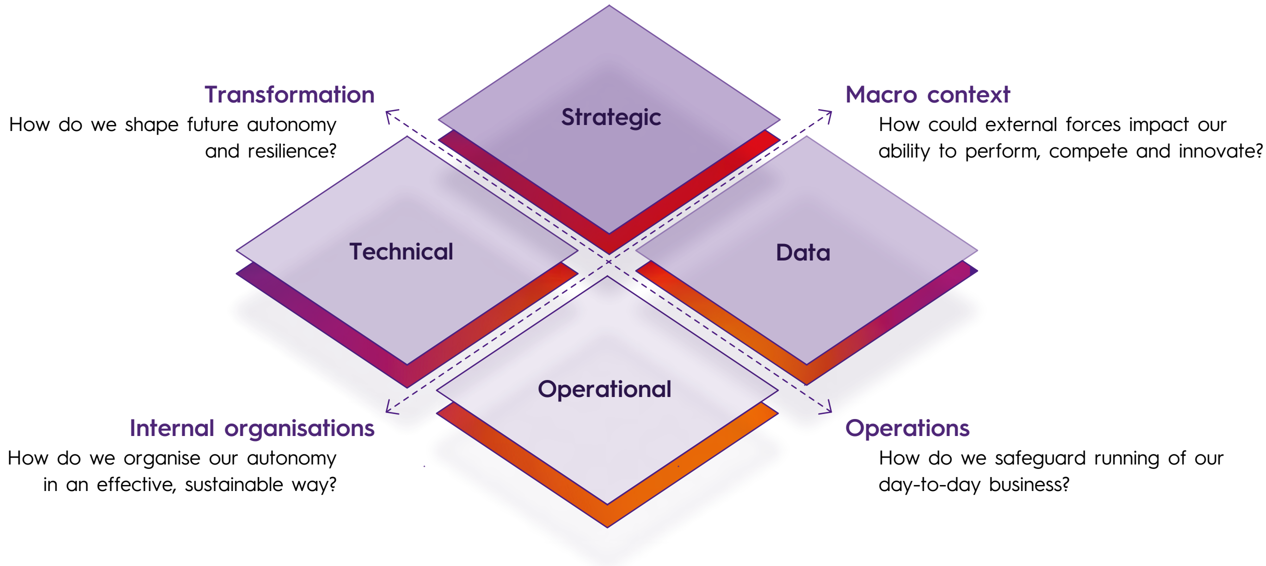
Joy van Baren
Portfolio Director, Sopra Steria Benelux

Our Framework: Four dimensions of digital sovereignty

Digital sovereignty is an imperative: a way to take control of your digital future before someone else does. But it's not just about protection; it's also about innovation. Can you access the exponential technologies that drive competitive advantage while maintaining control?

The answer varies by organisation, based on different risks, dependencies, and trade-offs. At Sopra Steria, we use a comprehensive framework to guide organisations on their sovereignty journey.

Four dimensions of digital sovereignty



Strategic sovereignty

It starts at the top: efforts to increase your autonomy and resilience can only be effective when sovereignty is prioritised and embedded in your business strategy.

Strategic direction
Have you defined what digital sovereignty means for your organisation, and determined your risk tolerance? Do you know which external factors could impact your autonomy? Have you mapped how your competitors are responding?

Prioritisation & embedding
Is sovereignty prioritised in your business strategy, and used to calibrate your long-term vision? Does it cascade into your digital strategy, data strategy, platform strategy, and so on?

Data sovereignty

Your digital services need to be designed and operated by you, instead of depending on black-box platforms or external orchestration. Your ability to control your data and meet compliance requirements increases resilience and helps you leverage AI.

Data strategy
Is your data strategy aligned with national, organisational, or citizen interests, or dictated by external vendors, platforms, or foreign regulations?

Data governance
Who defines and enforces the rules for data access, quality, sharing, and use? Are governance policies and frameworks aligned with local regulations, such as e.g., GDPR and AI Act?

AI governance
Do you have full control over how AI systems are designed and governed, including decision logic, ethical alignment, legal compliance, and infrastructure?

Technical sovereignty

Sovereignty needs to be embedded in your entire technology stack. This starts by mapping your exposure. What could break, and how easily could you adapt or shift? But also: do you have access to exponential technologies that help you innovate?

Cloud & infrastructure
Do you know your footprint and which jurisdictional risks apply? Are you dependent on non-EU providers? Could you exit without disruption?

Data storage & processing
Where's your most sensitive data? Who can access it, and under which laws? Are you ready to be audited?

Applications
Where are the dependencies in your application landscape, from vendor lock-in to lack of code or audit access, or even complete loss of access? How modular is your architecture?

IT Ecosystem
Are your suppliers aligned with your resilience goals, or just your procurement KPIs? Who are sovereign partners and providers that can accelerate your innovation agenda?

Operational sovereignty

Sovereignty fails without structure and integration into your day-to-day business. Response plans that work under pressure make the difference between resilience and regret. And you need people with the right awareness and skills, as well as physical proximity.

Governance
Can your organisation make fast, local decisions when sovereignty is at stake? Who decides what's critical, and what the escalation paths are?

Response plans
Could you recover quickly if a third party suddenly cuts access to your systems? How will you navigate disruption when you don't control the infrastructure?

Workforce
Do you have local capabilities to ensure continuity of your critical processes and systems? Do your people have the knowledge and skills to respond with confidence when it counts?

Legal
Do you have reliable access to local legal expertise? Can you comply with current requirements and adapt quickly when rules change?

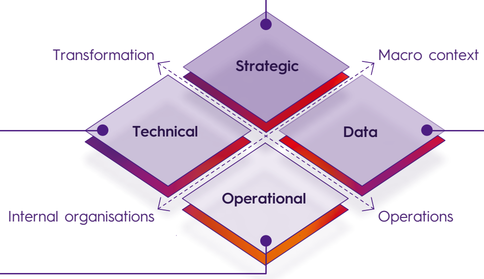
Increasing resilience in every dimension

Technical

- Evaluate hybrid or sovereign cloud set-ups, e.g. OVHCLoud. Align with European sovereignty initiatives (e.g. GAIA-X).
- Map data locations, enforce geo-fencing. Localise sensitive data, implement encryption, maintain audit logs.
- Prioritise transitioning sensitive workloads to open portable and sovereign applications. Negotiate code access and audit rights. Implement modular architectures to enhance control.
- Assess contracts for legal exposure and vendor lock-in. Build in exit options. Prioritise long-term strategic fit and innovate capacity.

Strategic

- Analyse external forces that could impact your ability to operate, compete or innovate.
- Define your strategic course. Benchmark against competition
- Prioritise sovereignty in your business strategy, ensure cascading to other areas.



Data

- Classify data for sensitivity and design for auditability.
- Implement data governance with lineage, access controls and complicance monitoring.
- Set-up AI governance to safeguard that AI is developed and used in line with your values, laws and strategic interests.
- Leverage European GenAI platforms such as Mistral or tailor-made versions of Sovereign Cloud.

Operational

- Incorporate sovereignty into your governance, empower teams to act and set clear escalation paths.
- Write and test response plans for impactful events.
- Build crossfunctional awareness across IT, legal, ops and procurement.
- Rethink your workforce to ensure essential capabilities are are physically close and under your jurisdiction

Our recommendations

Digital sovereignty doesn't have to happen all at once. What's important is knowing what to prioritise, where to act first, and how to stay accountable under pressure.

We guide you through **three focused steps**:

1. **Define priorities.** Get a clear view of which processes and systems are strategically most important and where autonomy is essential.
2. **Assess risk.** Identify which exposures threaten your compliance, operations, or strategic autonomy and understanding where dependencies lie.
3. **Build your roadmap.** Sequence changes based on urgency while aligning with longer-term regulatory requirements.

"Europe's future cannot be left to a handful of platforms. A resilient ecosystem needs diversity, combining global scale with local innovation. Digital sovereignty is urgent. I am proud that Sopra Steria creates digital infrastructure for organisations that is strong, fair and human."

Ernst-Jan Stigter
CEO Sopra Steria The Netherlands

Reclaim our digital destiny

Digital sovereignty expands choice, rather than limiting it. It gives us an exciting opportunity to design for responsible growth, with systems rooted in trust, not dependency or isolation.

Whether you're mapping exposures, rethinking cloud strategy, or re-designing for sovereignty from the ground up, Sopra Steria is ready to help. We can help you take back control where it matters.

Why Sopra Steria

We are your trusted partner for digital sovereignty, combining compliance, control, and performance without lock-in or delay. Built for continuity, alignment, and strategic independence.

Locally rooted
Fluent in European languages, national regulations, and cultures, always.

European by design
Fully European-owned with deep ties to regional universities and innovation partners.

Technology-neutral
We work across platforms to design end-to-end solutions that fit your context and preferences.

Trusted in critical environments
We have a proven track record where the stakes are high, helping European organisations to stay secure, sovereign, and in control.

Sopra Steria supports national ministries, public agencies, and strategic enterprises across Europe, including in defence (*French and Dutch Ministry of Defence*), public finance and banking (*BNP Paribas, Financial Intelligence Unit NL, De Volksbank*), and critical infrastructure (*ProRail, Tennet*). We also contribute to the securing of the Schengen Area and broader European digital resilience.

Sources

[1] European Parliamentary Research Service, 2024: *Digital Sovereignty in the EU* (Briefing 757632); https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf

[2] Human Rights in Finance, 2025: *HRIF.EU urges EU Financial Institutions with DORA-briefing*; https://hrif.eu/en/2025/02/hrif-doraukhttps://hrif.eu/en/2025/02/hrif-dora-uk/

[3] PrivacyCompany, 2022: *New risk assessment for Microsoft Teams, OneDrive and SharePoint Online in the public sector*; https://www.privacycompany.eu/blog/new-dpia-for-the-dutch-government-and-universities-on-microsoft-teams-onedrive-and-sharepoint-online

[4] Reuters, 2025: *Dutch parliament calls for end to reliance on US software*; https://www.reuters.com/world/europe/dutch-parliament-calls-end-reliance-us-software-2025-03-18/

[5] Tech Radar, 2025: *Denmark wants to replace Windows-and Office*; https://www.techradar.com/pro/denmark-wants-to-replace-windows-and-office-with-linux-and-libreoffice-as-it-seeks-to-embrace-digital-sovereignty

[6] Proximus, (n.d.): *Your data, stored and protected in full compliance with EU rules*; https://www.proximus.be/en/id_b_cl_eu_ compliant_data/companies-and-public-sector/news/news-blog/solution-news/eu-compliant-data.html