PANOP

PANOP RESEARCH · DIGITAL SOVEREIGNTY

Digital Sovereignty: Why, What, How

A short working paper for organisations buying cloud, communications and AI services in Europe: why sovereignty moved from politics into procurement, what the term covers once it is broken into measurable parts, and which controls actually change who can reach your data. Built on the European Commission Cloud Sovereignty Framework, the Government of Canada data sovereignty white paper, and published Swiss and UK market evidence.

EDITION SEPTEMBER 2026

PANOP RESEARCH · PANOP.IO

PANOP

01 · WHY

Sovereignty is now a procurement requirement, not a political position

Three things changed at the same time. Buyers learned that where data sits does not decide who can compel it. Public bodies began scoring sovereignty inside tenders, with a floor below which a bid is rejected outright. And boards started treating foreign dependency as an operational risk alongside cyber. The open question is no longer whether to hold a position, but which level to buy and for which data.

WHAT IS DRIVING THE SHIFT

LEGAL

Extraterritorial law

The CLOUD Act reaches the provider, not the building.

MARKET

Buyers score it

Brussels grades cloud tenders on eight sovereignty objectives.

RISK

Concentration

One provider can carry mail, identity, voice and AI for a sector.

THREAT

Rising incident load

The UK NCSC reports roughly a 50% rise in attacks over 2024-25.

AI

Conversations are data

Voice, prompts and transcripts are now training data.

THE EVIDENCE, IN NUMBERS

Enterprises with a sovereignty strategy	More than 75% by 2030, on Gartner's forecast
Geopolitics and provider choice	61% say it will increase their use of local or regional providers
Swiss infrastructure preference	Hybrid cloud is the preferred model in the 2026 MSM Research survey
EU public procurement	Eight objectives, five assurance levels, scored since October 2025
Canadian federal position	Public cloud permitted only up to Protected B, residency directed in policy

Read it this way. Sovereignty has stopped being a values debate and become a specification. The organisations that struggle are the ones asked to evidence it after the contract is signed.

Sources [4] Gartner and UK NCSC figures as quoted in BTL, Sovereign Communications, 2025. [1] European Commission, Cloud Sovereignty Framework v1.2.1, October 2025. [3] MSM Research for Swisscom, Digital Sovereignty in Switzerland, 2026. [2] Treasury Board of Canada Secretariat, Data Sovereignty and Public Cloud, 2018, revised April 2026. Full citations on page 5.

PANOP

02 · WHAT

Residency answers where. Sovereignty answers who can compel

Three terms are used as if they were one. Security keeps data from people who should not have it. Residency fixes the place it is stored. Sovereignty decides whose law and whose staff can reach it. A provider can satisfy the first two completely and still be obliged to hand data to a foreign authority, sometimes without telling the customer.

THE SOVEREIGNTY LADDER, AS THE EU SCORES IT

SEAL-0	SEAL-1	SEAL-2	SEAL-3	SEAL-4
No sovereignty	**Jurisdictional**	**Data**	**Resilience**	**Full**
Exclusive non-EU control, governed outside EU law.	EU law applies on paper; enforceability is limited.	EU law enforceable, material non-EU dependencies remain.	EU actors hold real influence; non-EU control is marginal.	Complete EU control, subject only to EU law.

THE EIGHT DIMENSIONS BEHIND THE SCORE

Strategic	Ownership, financing and decision authority anchored in the EU
Legal and jurisdictional	Exposure to the US CLOUD Act, Chinese Cybersecurity Law and similar reach
Data and AI	Customer-only control of keys, confined processing, verifiable deletion
Operational and supply chain	EU staff can run the service unaided; critical components traceable
Technology, security, sustainability	Open interfaces and audit rights, security run inside the EU, energy dependency

> **Read it this way.** Ask a provider for its assurance level on each objective, not for a sovereignty badge. One label hides the single dimension where control is missing, and that is the one that will be tested.

Sources [1] European Commission, Cloud Sovereignty Framework v1.2.1, October 2025: objectives SOV-1 to SOV-8, assurance levels SEAL-0 to SEAL-4. [2] Treasury Board of Canada Secretariat: definitions of data sovereignty and data residency. [6] Gaia-X, CIGREF, ENISA, NIS2 and DORA, as named in [1]. Full citations on page 5.

PANOP

03 · HOW

Five controls set the level, and each one costs something

Sovereignty is bought in increments, not declared in a policy. Each control below raises assurance on one dimension and takes something away on another: functionality, supplier choice, or operating burden carried in-house. The work is deciding which class of data justifies which control, then writing that into the contract before the renewal rather than after an incident.

THE FIVE MOVES, IN ORDER OF EFFORT

01	02	03	04	05
Classify first	**Hold the keys**	**Write it down**	**Local operation**	**Keep an exit**
Canada caps public cloud at Protected B.	Encrypt with keys the provider cannot use; processing is the gap.	Clauses compelling disclosure of access, where notice is lawful.	A national operator or a certified host, as in Germany and Australia.	A tested migration path keeps the other four negotiable.

WHAT EACH CONTROL FIXES, AND WHAT IT LEAVES OPEN

Data residency	Keeps data in country; does not stop foreign law reaching the provider
Customer-held keys	Makes data opaque to the provider; it must still be decrypted to be processed
Certification, ISO 27001 and C5	Evidences security controls; says nothing about jurisdiction
Contractual disclosure clauses	Creates notice and recourse; some orders forbid notification outright
Trusted operator or certified host	Puts access under national control; narrows the supplier market

Read it this way. No single control delivers sovereignty. Residency without key control is geography, and key control without an exit is dependency with better encryption.

Sources [2] Treasury Board of Canada Secretariat, Data Sovereignty and Public Cloud: mitigations and Appendix A comparison of government responses. [1] European Commission, Cloud Sovereignty Framework v1.2.1: contributing factors for SOV-2, SOV-3 and SOV-4. [5] Australian Government Digital Transformation Agency, Hosting Certification Framework. [6] UK NCSC, Cloud Security Principles, principle 2. Full citations on page 5.

PANOP

04 · IN PRACTICE

Six jurisdictions, six different settlements

The same legal risk has produced very different answers, and comparing them is the quickest way to locate your own position. Each example trades one thing for another: supplier choice, cost, operating burden, or speed of access to new technology. None of them claims to remove foreign reach entirely.

WORKED EXAMPLES

EU	CANADA	AUSTRALIA	GERMANY	UK	SWITZERLAND
Scored procurement	**Classify and cap**	**Certify the host**	**Trusted operator**	**Risk-managed**	**Hybrid by default**
Minimum level per objective gates the bid; the score ranks it.	Public cloud to Protected B; keys held by government.	Data must sit in certified assured or strategic facilities.	Hyperscaler platform, national telco controls access.	No blanket residency rule; NCSC principles guide it.	Sovereign workloads held beside global services.

REFERENCES, AND WHAT EACH ONE SUPPLIED

[1] European Commission	Directorate-General for Digital Services, Cloud Sovereignty Framework, version 1.2.1, October 2025. commission.europa.eu. *Supplied the eight objectives and the SEAL levels on pages 3 and 4.*
[2] Government of Canada	Treasury Board Secretariat, White Paper: Data Sovereignty and Public Cloud, 2018, page revised 23 April 2026. canada.ca. *Supplied the definitions, the Protected B cap and the mitigation table.*
[3] Swisscom, MSM Research	Digital Sovereignty in Switzerland, white paper, 2026. swisscom.ch. *Supplied the Swiss hybrid finding; the full text is gated, so only the published summary was used.*
[4] BTL	Sovereign Communications: what is it and why is it important, white paper, 2025. btlnet.co.uk. *Source of the Gartner and NCSC figures, quoted second-hand rather than from the originals.*
[5] Australian Government	Digital Transformation Agency, Hosting Certification Framework, April 2021, current 2026. hostingcertification.gov.au. *Supplied the certified assured and certified strategic model.*
[6] Frameworks named in [1] and [2]	Gaia-X policy rules; CIGREF Trusted Cloud Referential v2; ENISA, NIS2, DORA; UK NCSC Cloud Security Principles; BC OIPC cloud guidelines. *Cited as referenced by the primary sources; not consulted separately.*

Citation practice. Numbers in square brackets on pages 2 to 4 point to this list. Vendor figures are marked where they are quoted second-hand.

Method *All sources are public documents; web pages accessed September 2026. Where a figure originates with a third party quoted inside a vendor paper, the quoting document is cited and the origin named in the text.*