Sovereign-Cloud-Washing: Five Questions

2026-07-09

Five questions on jurisdiction, technical access, key control, exit paths, and switching cost to test any ‘sovereign cloud’ claim beyond marketing. Part 1 of 6.

“Sovereign cloud” is printed on marketing pages from AWS, Microsoft, Google, and a long list of European providers alike. The label rarely comes with a definition, which makes it easy to satisfy on paper and hard to verify in practice. I’ve put together five concrete questions, asked of the claim itself instead of the label — enough to see, from several angles, what a provider actually stands behind.

i What you

Five questions for testing a sovereignty claim: legal ownership and jurisdiction (acknowledged here as a legal question, not an engineering one); who or what actually has technical access to the system; whether protection is legally-enforced or technically-enforced; whether a real exit path exists; and what it costs to switch — to a cloud, between clouds, or back to on-prem — at all. Illustrated with findings from provider research already published on this blog, plus a closing checklist to apply to any provider.

⚠ Not a legal opinion

The ownership, jurisdiction, and corporate-structure details below come from public sources — press releases, company registries, news coverage — gathered while researching infrastructure decisions from a technical, engineering angle. The legal and sovereignty questions surfaced along the way; they were not the starting point, and I am not a lawyer. Treat this as a technical framework that happens to touch on ownership and jurisdiction, not a legal assessment. If sovereignty status is load-bearing for an actual decision, that needs review by someone (or a team) qualified to assess it from a legal perspective — this post is not a substitute for that.

Question 1: Who legally owns this, and under what jurisdiction?

A sovereignty claim usually starts with a jurisdiction promise: incorporated in the EU, data stored in an EU datacenter. That covers only the entity making the claim — not who sits above it in the ownership chain, which can run through a parent company, a private-equity owner, or a holding structure several layers up that the marketing page never mentions.

Answering this rigorously is a legal question, not an engineering one — tracing an ownership chain and judging what it means for jurisdiction is corporate-law and compliance territory, not

something this blog has the expertise to assess. What it can responsibly say: ask the question, and route it to legal or another qualified person, rather than taking a jurisdiction claim at face value. A few ownership chains found while researching infrastructure providers for an unrelated technical comparison make the point plainly — a marketing page would never surface any of these on its own:

Provider	What the ownership chain actually runs through
Contabo	Majority-owned by KKR (US) since June 2022, with prior investor Oakley Capital (UK) retaining a minority stake
servers.com	Sits under CloudOne Digital, formed in 2023 by One Equity Partners, a US private-equity firm spun off from JPMorgan Chase
Exoscale	Its Swiss/Austrian entities sit under A1 Telekom Austria Group, which is 60.8%-owned by América Móvil (Mexico) — an "EU parent" that isn't itself EU-controlled
Gridscale	A German-founded brand, wholly owned by OVHcloud (France) since 2023 — a reminder that "pick a German alternative" can land back on the same company being avoided

Sources: OVHcloud newsroom on the Gridscale acquisition, One Equity Partners on forming CloudOne Digital, Oakley Capital on its Contabo exit to KKR, Telekom Austria's 2018 acquisition of Exoscale, and América Móvil's 60.8% stake in A1 Telekom Austria (Sept. 2025).

Question 2: What's the technology supply chain, and who — or what — has access to it?

Legal ownership is one layer; the technology stack running underneath it, and who can actually reach it, are separate layers again — and none of them automatically line up.

The supply-chain layer. Open Telekom Cloud is one illustration: legally owned and operated by Deutsche Telekom, which checks the ownership question cleanly, while the platform itself launched as an OpenStack-based service explicitly marketed as "powered by" Huawei, with a Huawei whitepaper naming FusionSphere as the underlying platform. Deutsche Telekom operates the service, but the exact current hardware/software stack is not public — a 2025 press interview shows the topic remained publicly debated that year. Clean legal ownership does not, by itself, answer what the platform is built on. Further examples of this same pattern, from other providers, are the subject of Part 2 of this series.

The access layer. The same question applies one level down, to who or what can actually touch the system day to day — provider support staff with break-glass access, third-party managed-service contractors, and increasingly AI agents given API or console credentials to operate infrastructure on someone's behalf. A sovereignty claim about where data legally sits says nothing about whether that access is documented, whether it is logged and auditable, or whether it is technically scoped — time-limited credentials, least-privilege roles, restrictions on what an autonomous agent can reach — rather than resting on a policy that says access "should" be limited. A platform can be fully EU-owned, EU-built, and still leave this question open.

Question 3: Is protection legally-enforced or technically-enforced?

This is the technical-enforcement side of the access question above: not just who is *supposed* to have access, but what actually stops them, and how, if the policy answer ever fails.

A jurisdiction promise is a legal statement: "we are EU-incorporated, so this data is not subject to a foreign government's reach." Legal statements carry weight, but they describe a policy position — one that can be tested, reinterpreted, or overridden by future legislation, corporate restructuring, or a court ruling the provider did not anticipate. The extraterritorial reach of the US CLOUD Act, and comparable regimes such as FISA Section 702, is unresolved enough in practice that providers reasonably differ on how much protection incorporation location actually buys.

A technical guarantee is a different kind of claim: the provider is architecturally incapable of reading the data, regardless of what any court orders it to do. Customer-held encryption keys (BYOK — bring your own key) are the clearest version of this. Comparing BYOK support across AWS, GCP, Azure, and OVH — done for an unrelated log-archiving cost and security comparison — found all four support some form of customer-managed keys, with meaningfully different operational models. AWS KMS and Azure Key Vault keep the key inside a managed service whose lifecycle the customer controls. OVH's SSE-C model goes further: the customer supplies the raw encryption key on every single API request, and OVH's own documentation states plainly that if the key is lost, the data becomes permanently unreadable — because OVH itself never stores it.

That's the difference in practice: not "we promise not to look," but "we cannot look, because we do not have the key." A legally-enforced promise depends on the promise holding up; a technically-enforced one does not depend on anyone keeping a promise at all. The full provider-by-provider BYOK comparison is in Log Archiving Security & Compliance — Part 4.

Question 4: Can you leave?

The first three questions test the sovereignty claim as it stands today. This one tests what happens the day any of those answers change — an acquisition, a shift in a company's legal domicile, a change in an export-control regime. A provider whose data model exports in a standard format, whose ingest and query APIs are not proprietary, and whose egress pricing is not structured to punish moving data out, gives a customer a real exit path if the sovereignty picture changes later. A provider that answers the first three questions well but locks data behind a proprietary format or steep egress fees is offering sovereignty as a snapshot, not a standing property — good until the day leaving becomes the point.

This question gets its own dedicated deep-dive in Part 5 of this series; here it stays deliberately general.

Question 5: What does it cost to leave — or to arrive?

On-premises infrastructure is largely sovereign: there is no third party to ask a jurisdiction or access question about. The exceptions are the vendors of the products in use, which may require access to the systems. That makes it tempting to treat "stay on-prem" as the default answer and everything else as a compromise — but only for as long as the organization can — or wants to, or in some regulated cases simply must — keep bearing the ongoing cost of that choice. And that isn't theoretical: Broadcom's acquisition of VMware has sharply raised licensing costs on exactly that

widely-used virtualization platform over the past months and years. The cost of the move itself is usually underestimated — in either direction. Migrating to any cloud, moving between clouds, or partially staying on-premises all carry real switching costs: engineering time re-architecting for a new platform's primitives, process changes in how deployments, backups, and incident response work, and costs not known upfront at all, which only surface during the move itself — for instance where a lock-in clause or an egress fee makes the switch to another vendor hard to estimate.

The human component sits inside this same question, not beside it: a switch is only as fast as the team's ability to operate the destination platform, and a sovereignty decision that looks clean on a slide can stall for months on a skills gap no one accounted for. A provider or platform that scores well on the first four questions but requires rebuilding operational competence from scratch is not offering a free move — the costs, known and unknown, shift to after the migration, or only become visible in the middle of it.

Like Question 4, this one gets its own dedicated deep-dive — in Part 6 of this series; here it stays deliberately general.

A checklist, not a ranking

The five questions, condensed into something to run against any provider making a sovereignty claim — a checklist, not a scorecard for ranking specific vendors:

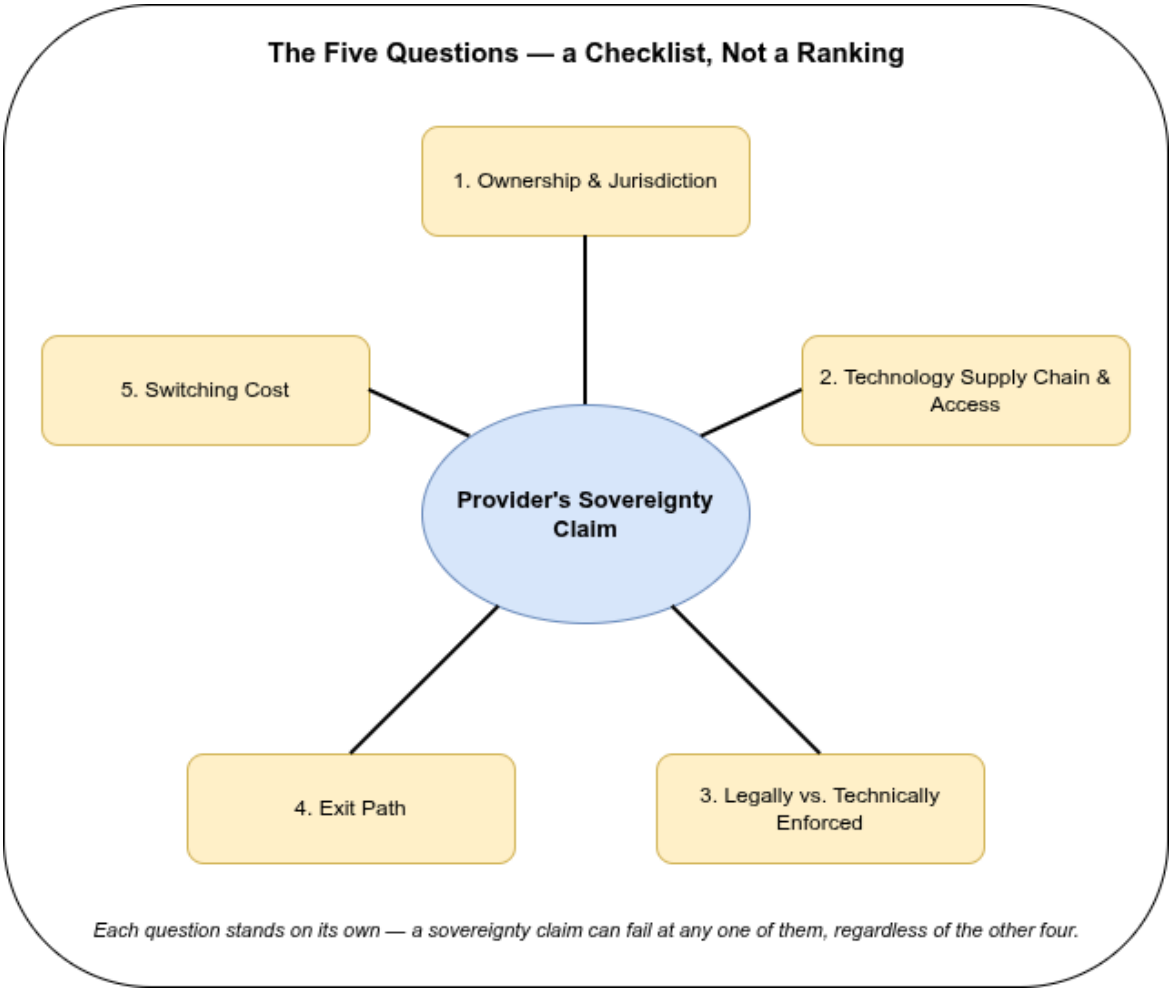

Figure 1: Diagram: the five sovereignty questions arranged as equal spokes around a central sovereignty claim — a checklist, not a ranking

Question	What to check	A claim worth being skeptical of
1. Ownership & jurisdiction	Corporate registry, parent-company press coverage, M&A history — or better, ask legal	"EU-incorporated" stated without addressing who owns the entity above it
2. Technology supply chain & access	Platform/hypervisor vendor and licensing; who (staff, contractors, AI agents) has access, and whether it's logged and scoped	Ownership confirmed EU, but the platform vendor is undisclosed, or access is undocumented
3. Legally- vs. technically-enforced protection	Whether encryption keys are customer-held (BYOK) by default, or platform-managed	"We don't share data with governments" with no mention of who holds the encryption key
4. Exit path	Data export format, API openness, egress pricing	A proprietary format or punitive egress fees paired with a sovereignty claim
5. Switching cost	Re-architecture effort, process changes, contractual lock-in, team skills for the destination platform	A "sovereign by default" claim (e.g. staying on-prem) that ignores what the move itself would cost

“M&A” stands for “Mergers and Acquisitions”.

Using the five questions as a checklist like this, you can build your own scorecard and probe the cloud provider — or providers — of your choice with it. That gives you, as the responsible person, something tangible for yourself and for management, to check how and whether a specific provider fits your business.

None of these five questions has a single right answer that applies to every organization equally. A workload with no US-jurisdiction exposure at all may not need a technical guarantee layered on top of a legal one; a regulated workload under audit typically needs both. What changes the outcome is asking the specific questions and handling the answers honestly, instead of simply accepting the marketing statements. What naturally undermines all of this are statements already made, like “We’re moving to provider X.”

Next in this series: Part 2 — Who Builds the Platform? Ownership vs. Stack →

Related

- Log Archiving Security & Compliance — Part 4 — the BYOK and encryption-key comparison behind Question 3
- AWS vs. GCP vs. Azure vs. OVHcloud: Managed Log Archiving — Part 1 — where the CLOUD Act / FISA jurisdiction distinction first came up in the context of a cost comparison