

TechArena®

Verify, Don't Trust

What sovereign AI buyers
require now



By Rachel Horton
November 2026

Governments and regulated enterprises have moved sovereign AI from policy to procurement. The builders serving them say those buyers now require proof of control: where the infrastructure sits, who runs it, who can reach the data and how the buyer plans for what it cannot control.

Executive Summary

Sovereign AI has moved from policy to procurement, and the governments and regulated enterprises buying it answer to legislatures, regulators and national security processes. That accountability shapes what they require from the companies that build and run their AI infrastructure. This paper sets out four of those requirements, drawing on authoritative voices building sovereign AI infrastructure in Europe and beyond. Those requirements start with a working definition of control. From there, buyers require infrastructure whose location they can verify against a standard, along with operators and access controls they can audit, down to who holds the encryption keys. They also require a plan for the inputs no single buyer fully controls, from the supply of cutting-edge accelerators to access to frontier models. The paper closes with what a sovereign buyer should ask to see before signing.

THE FOUR REQUIREMENTS

01 Control they can define

02 A location they can verify

03 Operators and access they can audit

04 A plan for what they can't control

Proof, Not Promises

Mistral closed a €3 billion Series D on Sept. 8, 2026, the largest equity round ever completed by a European technology company.¹ The company plans to scale European compute capacity to 1GW by 2030 and to offer regional data processing to governments and companies that want AI independence from US providers. In late July, the EU opened its call for up to seven AI gigafactories, with €10 billion in public funds and at least €20 billion in expected private investment behind it.²

Capacity is only half of what sovereign AI buyers need. The builders serving them say those buyers also have to prove they control it.

“‘Trust us’ isn’t an acceptable answer to a government customer. ‘Here’s how you verify it yourself’ is,” said Nidhi Chappell, Nscale’s president of AI infrastructure. “That shift — from performance-first to verifiable-first — is the biggest change in how I design.”

The shift follows from who the customer answers to. Large hyperscalers design to optimize throughput, cost per token and uptime for a single company’s roadmap, Chappell said.

“‘Trust us’ isn’t an acceptable answer to a government customer. ‘Here’s how you verify it yourself’ is.”



Nidhi Chappell
Nscale

“Government and regulated entities aren’t just optimizing for performance — they’re accountable to a legislature, a regulator, or a national security process,” she said. “That changes the requirements: auditability, chain of custody for hardware and data, procurement cycles that need more time, and a need to prove things rather than simply deliver them.”

Who Is Buying, and Why Now

Sovereign buyers have moved from talk to action. Eighteen months ago, their posture was rhetorical, said Jonathan Symonds, chief marketing officer at Radiant, the vertically integrated AI infrastructure company Brookfield launched in February.³ Now, governments are executing.

“Sovereign nations are also much more serious than they were,” Symonds said. “They are openly putting RFPs into the market.”

The trend is strongest in Europe and extends to South Korea, the United Arab Emirates and Saudi Arabia. Those buyers want speed, a fast path to first production capacity and a clear roadmap to self-sufficiency, he said.

Export controls on AI models also put model providers, not just governments, in the market for compute.

“The first beneficiary of the export controls were other model providers with fewer political entanglements,” Symonds said. “Cohere and Mistral are excellent examples.”

Those model providers now shop for compute in ways they did not six to nine months ago.

Scaleway sells control without the sovereign label. Albane Bruyas, chief commercial officer and chief operating officer at the French cloud provider, avoids the word because its definitions vary so widely.

“What we sell more and what is very interesting for our clients is that we sell a full autonomy,” she said during a recent TechArena podcast. “This means that we have control on all the value chain. This is what makes the pure difference for our clients.”

SOVEREIGN AI BY THE NUMBERS

\$80B

Forecast 2026 spending on sovereign cloud IaaS, up 35.6% over 2025

GARTNER

75%+

European and Middle Eastern enterprises expected to geopatiate workloads by 2030, up from less than 5% in 2025

GARTNER

€30B+

Public and private investment behind the EU's call for up to seven AI gigafactories

EUROPEAN COMMISSION

Gartner forecasts \$80 billion in sovereign cloud infrastructure-as-a-service spending this year, a 35.6% increase over 2025, with governments as the main buyers.⁴ Gartner also expects more than 75% of European and Middle Eastern enterprises to geopatiate their workloads by 2030, moving them out of global public clouds and into local options, up from less than 5% in 2025.⁵ Nscale closed a \$2 billion Series C at a \$14.6 billion valuation in March.⁶

The US CLOUD Act lets American authorities compel US-headquartered providers to hand over data they hold abroad.⁷ Under that law, a provider's headquarters, not only the location of its data center, determines which government can demand a buyer's data. In Europe, the EU AI Act requires organizations that deploy high-risk AI systems to keep the logs those systems generate for at least six months, to the extent the logs are under their control. Those obligations take effect Dec. 2, 2027.

Control They Can Define

A buyer has to define control before it can verify it. Chappell defines it this way.

“For us, sovereignty means enabling governments and enterprises to run critical AI workloads under their own legal, operational and security frameworks — with clear control over where infrastructure sits, who operates it, who can access it, and which laws apply,” she said. “That’s not only about where data resides; it’s about control of the compute infrastructure underneath it.”

A sovereign can take more control over some inputs than others. Symonds ranks the inputs a sovereign needs, from data and land to models and compute, by how much control a sovereign can take over each. Data comes first.

"Data is the fuel," he said. "You wouldn't bother with sovereignty if you weren't starting from the data layer."

After data, Symonds ranks the remaining inputs in this order:

"Control what you can, invest there, reduce risk everywhere else."



Jonathan Symonds
Radiant

How much control can a sovereign take?

Jonathan Symonds' ranking of sovereign AI inputs, Radiant

MOST
CONTROL



LEAST
CONTROL

- | | |
|----|---|
| 01 | Data |
| 02 | Powered land |
| 03 | Running the system itself, or trusting the partner that runs it |
| 04 | Models |
| 05 | Build capability |
| 06 | Networking |
| 07 | Compute |

"You can own and operate the GPUs, but you cannot meaningfully control the upstream supply of cutting-edge accelerators," Symonds said. "One does not homegrow cutting edge GPU capacity overnight."

"Control what you can, invest there, reduce risk everywhere else," he said.

That rule orders a sovereign buyer's requirements. Buyers verify the inputs they control: where the infrastructure sits, who operates it and who can reach the data. They plan for the inputs they cannot fully control: accelerator supply, access to frontier models and the suppliers they depend upon.

A Location They Can Verify

Location is the first requirement a sovereign buyer verifies. In a standard public cloud region, Chappell said, "region" is often a configuration setting. Workloads and data can be routed, replicated or failed over across borders by default, and "a customer largely has to take the provider's word for where things actually run."

Nscale's partnership with BT takes a different approach.

"With BT, the sites, the network paths, and the operational access are fixed to UK jurisdiction and governed by BT's existing security and compliance frameworks, not a config toggle that could quietly change," Chappell said.

In practice, the physical location of the hardware is known, fixed and auditable. Data does not leave the jurisdiction as part of normal operation.

"The whole environment can be independently verified against a standard, rather than just asserted," she said.

Nscale matches location to the workload.

"Not every country needs its own hyperscale campus, so the model we're pursuing is federated," Chappell said.

Large training campuses sit where power is abundant and low-cost, in the Nordics and Iberia. Those campuses feed smaller in-region or in-country clusters for workloads that have to stay local. BT supplies the in-country half in the UK, with national telco infrastructure and sovereign compute layered on top, serving public sector and enterprise customers.

Location also depends on land and power, the physical inputs Symonds ranks highest.

"You can and should control your physical inputs," he said.

In a true sovereign sale, he said, the sovereign likely owns the land and the power. Radiant designs, builds and turns up the AI factory, finances it if needed and operates it up to a point.

Power is the requirement buyers most underestimate, Chappell said.

"Most sovereign programs plan the compute procurement first and the power second, and power is what actually gates the timeline," she said.

Nscale owns its power envelope, which changes how it designs.

"When you own the power envelope, you're not just backing into a wattage number after the fact," Chappell said.

Nscale designs density and storage placement around the actual power profile of each site from the start, and it throttles GPU draw dynamically rather than overprovisioning.

"Most sovereign programs plan the compute procurement first and the power second, and power is what actually gates the timeline."



Nidhi Chappell
Nscale

Operators and Access They Can Audit

The next set of requirements covers people. Symonds ranks self-operation second, right after powered land. A sovereign has to build the capacity to run its own system, even in phases, he said, or place true trust in an operating partner.

At BT, only vetted personnel operating under UK law can reach the control plane, Chappell said.

"Baseline, not premium," Chappell said. "In a sovereign or regulated context, those aren't things a customer upgrades into later — they're the entry requirement to even be considered for the bid. We don't access or inspect customer GPU workloads, and that isolation, alongside encryption, verifiable erase and firmware integrity, is built into every deployment, not sold as an add-on tier."

Access requirements extend to the data itself. In an air-gapped, on-premises build, weights and data persist at rest in the storage system. Symonds said the deciding question there is "who has technical authority over the storage system: who controls access, encryption keys, updates, telemetry and administrative privileges."

Most modern storage runs as software on standard server and flash hardware, Symonds said. He advises buyers to choose that software from a vendor they trust and architect it so the

sovereign operator, not the vendor, retains control of keys, access, software updates and external connectivity.

Vendor domicile still counts. Some countries will not buy storage from companies domiciled in certain other countries, Symonds said, and “that is a legitimate procurement and supply-chain consideration.” Domicile does not replace technical control.

“Vendor domicile and government exposure remain relevant risk factors, but they are not substitutes for those technical controls,” he said.

Auditing access gets harder outside the data center. Chappell calls extending real-time response to the edge, at the same security bar as the core, the hardest thing a sovereign builder has to deliver. A core facility takes some of its trust from physical design: badges, perimeters, cameras. An edge node lacks those by definition, “so you have to rebuild that trust in hardware and software instead of walls, at the same latency budget.”

“Physical security can’t be your only control once the node leaves the building.”



Nidhi Chappell
Nscale

“The underlying principle is that physical security can’t be your only control once the node leaves the building,” she said.

Proof does not replace trust in the provider. Symonds said Radiant’s customers know the company can deliver because it holds capital, powered land, compute access and software in house.

“They have confidence we are going to be around in 18, 36, 48 months,” he said. “In that sense, trust is another differentiator.”

A Plan for What They Can’t Control

A buyer that verifies every input it controls still depends on inputs it cannot fully control. Symonds expects compute to be the hardest constraint three years out. Hyperscalers, frontier labs and major AI enterprises will continue to absorb a disproportionate share of leading-edge capacity, he said. Most governments will build 50MW to 500MW in that window, and multi-gigawatt scale will elude almost all of them.

Those governments can build data centers and procure models, Symonds said. GPUs and the networking to keep them fed will be harder to secure unless buyers place orders well ahead of time. Public-sector procurement tends to value optionality and staged commitment.

"Getting things built favors the bold," he said.

Scarce compute raises the value of every GPU a buyer secures.

"Storage decides whether the expensive compute you've built actually gets used — that's a direct line to unit economics," Chappell said.

AI agents, software that plans and carries out multistep tasks with limited human direction, sharpen the problem. Agentic inference brings unpredictable access patterns as many agents hit shared context or memory stores at the same moment.

"Storage breaks first," Chappell said.

Under that load, peak demand matters more than the average.

"Architectures tuned purely to averages will look efficient on paper and fail live," she said.

Models are the second input a buyer cannot fully control. Discussing the US-China contest over model weights, Symonds reduced control to one test.

"This is all about control and, in this context, control is the ability to rescind access," he said.

Washington and Beijing increasingly regard the weights themselves as strategic technology, Symonds said. In his reading, China wants the ability to pull its free but very good models if the US pulls its expensive but cutting-edge ones. Open weights work the other way.

"Once the weights have been openly released, they are extraordinarily difficult to claw back," he said. "Open source models offer an opportunity for sovereigns to have real control and real personalization."

His advice to buyers: "de-risk your model supply chain now."

"This is all about control and, in this context, control is the ability to rescind access."



Jonathan Symonds
Radiant

Suppliers are the third. Digital buyers too often forget a rule the industry treats as basic, said Albane Bruyas of Scaleway. A company that depends on one strategic supplier has no fallback if that supplier fails, raises prices or receives a data request from a foreign government. In industry, she said, a buyer of a strategic component chooses at least two suppliers, so a fire at one factory still leaves somewhere to buy.

Open hardware makes the second supplier possible, she added. The more open the hardware, the more suppliers an operator can buy from, and more suppliers mean better prices and more capacity. Scaleway buys European when it can, because in her view purchase orders, not grants, build an ecosystem.

Owning the full stack reduces dependency from the other direction. Nscale owns its power, data centers, compute and software, which removes subcontractors from the chain a sovereign buyer has to trace. Radiant builds on the same model.

“Our core advantage was, and continues to be vertical integration,” Symonds said. “Others can match different components, capital, powered land, compute access and expertise, software, but no one yet has demonstrated the ability to unify them all.”

The TechArena Take

Verifiability now stands alongside performance as a requirement in sovereign AI procurement. We expect the sovereign builds of the next three years, most of them in the 50MW to 500MW range Symonds describes, to go to builders who can show a buyer, line by line, which inputs the buyer controls and how a third party can check each one.

A sovereign buyer should ask to see five things before signing

- 1 The standard against which the site's jurisdiction is independently verified.
- 2 The people who can reach the control plane and the law they operate under.
- 3 Who holds the keys, updates and telemetry for the systems where data and weights persist.
- 4 The power plan, before the compute order.
- 5 The plan for accelerator supply, model supply and a second supplier.

We see verification becoming part of the product itself. Builders that document jurisdiction, operator access and data control before the first workload runs give buyers what a legislature or regulator will ask to see. We expect those builders to turn sovereign RFPs into production capacity fastest. For sovereign AI buyers, proof is now part of what they pay for.

Sources

1. Anna Heim, "[Mistral raises €3B as sovereign AI becomes big business](#)," TechCrunch, Sept. 8, 2026.
2. European Commission, "[EU launches AI Gigafactories call to boost Europe's computing capacity and unlock more than €30 billion in investment](#)," July 30, 2026.
3. Deanna Oothoudt, "[Brookfield Bets on Sovereign AI With Radiant and Ori Deal](#)," TechArena, February 2026.
4. Gartner, "[Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total \\$80 Billion in 2026](#)," Feb. 9, 2026.
5. Gartner, "[Gartner Identifies the Top Strategic Technology Trends for 2026](#)," Oct. 20, 2025.
6. Nscale, "[Nscale Raises \\$2 Billion in Series C — the Largest in European History](#)," press release, March 2026.
7. Jennifer Daskal, "[Unpacking the CLOUD Act](#)," eucrim.



TechArena 2026

© TechArena 2026. Other names and brands are property of their respective owners.