

The Sovereignty Stack

What's Actually Sovereign

Most “sovereign AI” vendors won't tell you where their claims end.

We will.

Simply because that's the only kind of sovereignty claim that survives regulatory scrutiny, and the only kind worth building a SOC on.

Why Sovereignty Claims Are Under Scrutiny

A 2026 Tech Policy Press / AI Now Institute analysis found that most European “sovereign AI” claims collapse under scrutiny because vendors are running proprietary US models bundled with hyperscaler contracts, or building inference capacity that ultimately subsidizes the same US labs it was meant to counter.

Sovera is built differently: an open-weight Mistral model, fine-tuned and served on Sovera-owned GPUs, inside a Sovera-controlled EU data center, wrapped in a purpose-built agentic framework for security investigations. Industry analysts call this “compute sovereignty”: owning the critical inference infrastructure rather than renting access to it. It's a narrower, harder claim than “we use a European model.” It's also the one that actually matters for NIS2 and DORA-regulated buyers.

“Sovera runs an open-weight Mistral model on our own GPUs, in our own EU data center, wrapped in an agentic framework with built-in authentication, segregation of duties, and approval controls. No hyperscaler sits in the model-serving or customer-data path, and every investigative action is auditable.”

The Stack, Layer by Layer

We could call all of this “sovereign.” We won't. Here's exactly what Sovera controls and what we don't.

STACK LAYER	SOVERA CONTROLS	STATUS	WHAT THIS MEANS FOR YOU
Model weights / architecture	Open-weight Mistral model	Partial	Built on an open-weight model from Mistral (France/EU), not a proprietary US model. Sovera doesn't control the original training data or pre-training compute.
Fine-tuning / adaptation	Mistral-controlled	Partial	Handled by Mistral, an EU company but not Sovera.
Prompt optimization	Sovera-built, in-house	Sovereign	Proprietary pipeline built and owned by Sovera, tuned specifically to improve accuracy in agent-driven security investigations
Agentic framework- Governance & audit	Sovera-built, in-house	Sovereign	Role-based control over who can generate a report, approve findings, or isolate a host with full rollback. Maps directly to NIS2/DORA access-control and auditability requirements..
Inference / model serving	Own GPUs, own data center	Sovereign	No hyperscaler in the inference path. This is critical because your data never leaves infrastructure Sovera owns and operates.
Physical hardware (GPUs)	Owned, not rented	Partial	The hardware is ours but the silicon itself is a US supply-chain dependency shared by every vendor in the industry, not a Sovera-specific gap.
Data center / facility	EU-located, Sovera/partner-operated	Sovereign	Located and operated within the EU. Jurisdiction and physical access control both stay on European soil.
Customer data processing & storage	EU jurisdiction	Sovereign	Core GDPR/NIS2/DORA guarantee: your data doesn't transit or get cached on any US cloud service, at any point.
Corporate structure & jurisdiction	Copenhagen HQ, EU entity	Sovereign	Legal domicile and governance sit fully in the EU — meeting NIS2/DORA procurement requirements that offshore vendors can't.

Let’s Put it to the Test

No hyperscaler path, EU jurisdiction, full audit trail, and radical transparency.

Want to see how sovereign MDR fits your environment? **Let's start with a conversation, not a claim.**