UNDERSTANDING DATA SOVEREIGNTY IN EUROPE

CMA INTELLIGENCE

enreach

Historically, data sovereignty had been a specialist concern, a line item towards the bottom of RFIs. It mattered deeply in some corners of the market, particularly in highly regulated industries and public sector environments, but in many sales conversations it was an afterthought. That is changing.

A Gartner survey of CIOs and IT leaders in Western Europe in November of 2025 revealed that **only 2%** felt that geopolitics would not increase their future use of local and regional cloud providers and **only 8%** felt that geopolitical issues would restrict their future use of global cloud vendors.[1] Across Europe, sovereignty has skyrocketed to the front of customer conversations.

Sovereignty has stopped being about ticking the compliance box. It has expanded into a required proof point that shows a vendor's understanding of the customer's unique environment and needs. It's about knowing the market into which the vendor is selling, and its unique nuances. The question isn't ***"can we comply with GDPR?"*** it's ***"Is this a market that you understand, are fully committed to, and can deliver in?"***

This requires a higher standard from service providers, vendors, partners, and the larger ecosystem. Customers are asking broader, sharper questions. They want to know not only where their data is stored, but how it is processed, who can access it, which laws may apply to it, what third-party services sit in the stack, and whether the provider truly understands the local operating environment in which the solution will be used.

That is a much bigger conversation than ***"is the data in Europe?"***

SOVEREIGNTY IS NO LONGER JUST ABOUT DATA LOCATION

One of the most important shifts in the market is that sovereignty is no longer being defined purely by where data resides. Data location still matters, of course, but it is now only one part of a wider set of concerns.

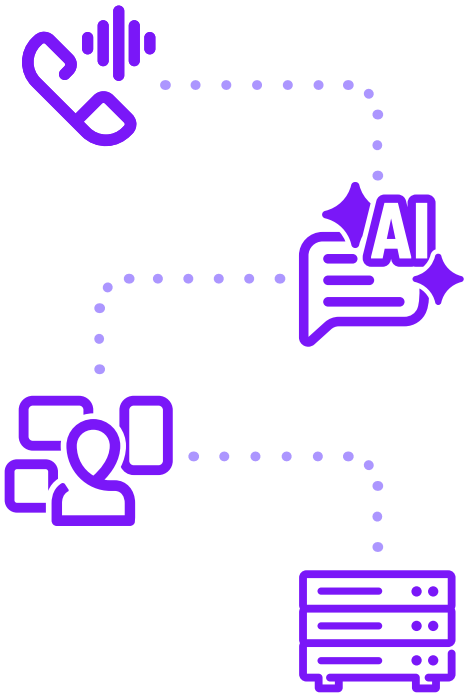
IDC's European research shows that protecting against extra-territorial data requests is now the leading sovereign cloud driver in Europe, but that is only one part of a wider sovereignty picture shaped by geopolitical risk, legal exposure, dependency, and autonomy.[2]

Customers expect sellers to be comfortable leading that discussion. They are becoming more aware of the challenges around data use, access controls, sub processors, legislative exposure, corporate structure, and third-party technology embedded in the service.

They will not accept vague reassurance, nor do they want a seller who visibly tries to sidestep the topic because it feels awkward or complex. They want confidence that the provider understands the issue, can walk them through their specific nuances, and has a solution built for their market, shaped around its realities, and capable of driving value within them.

In practice, that means sovereignty now includes operational control, vendor nationality, process compliance, legislative compliance, and traceability across the full service chain. This is especially important in our industry, where data flows across multiple systems. Voice recordings may be ingested into the CRM. AI services may sit behind transcription, summarisation, routing, or automation workflows. Middleware, APIs, and workflow tools may pass data between multiple vendors. On paper, each element can appear manageable. In practice, the full chain is often far harder to map than many organisations realise.

That is why sovereignty can no longer be treated as a box-ticking exercise. It has become a question of whether the seller can demonstrate real understanding, real comfort with the complexity, and real credibility in the customer's environment.



"The question is not only where data is stored, but how it moves and who touches it."

EUROPE IS NOT ONE SOVEREIGNTY MARKET

It is also important not to oversimplify Europe.

There are EU-wide regulations. There are country-specific laws. There are EU directives interpreted and applied differently across national markets. There are also vertical-specific expectations, contractual requirements, local practices, and in some countries, strong collective bargaining and labour environments that can create highly specific operational requirements at the company level. All of this shapes how a solution must be deployed and operated in the real world.

Customers don't want a vendor that merely complies with current requirements. They want one that understands how those requirements are evolving, can apply learnings from other European markets that might have advanced further in certain aspects, and can help them stay ahead of the direction of travel.

A provider may appear strong on paper from a data sovereignty perspective and still struggle in practice if it does not understand country-specific requirements, local business norms, language expectations, or cultural realities. Sovereignty is not just about where a platform is hosted. It is about whether the provider can operate in a way that aligns with local expectations and restrictions.

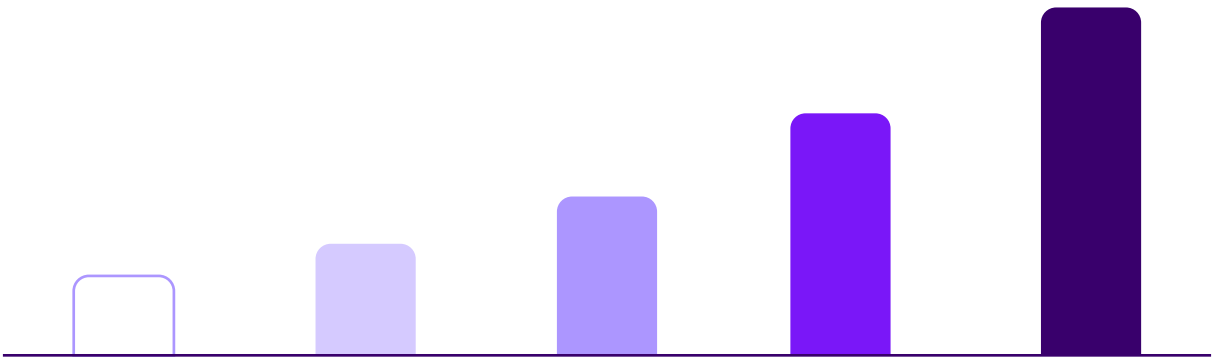
A partner that does not understand these realities may find that a seemingly compliant solution still fails the customer's real-world requirements. The European market needs to be approached with much more nuance. "European sovereignty" is not a single requirement set. It is a layered combination of EU-level, country-level, and vertical-level concerns. The onus is on the seller to educate and lead the customer.

SOME BUYERS CARE MORE THAN OTHERS

Larger organisations tend to ask more detailed questions. Organisations close to the state, including local government and public-sector-adjacent bodies, are often much more demanding. Healthcare and financial services remain especially sensitive. Telcos are another standout category, often looking not only at where data sits, but at infrastructure provenance, software provenance, deployment model, and the wider control environment. Customers operating across borders often face a competing mess of national regulations to decipher.

For partners, the sales motion must adapt accordingly. A non data sensitive mid-market organisation in one country may still be comfortable with a much lighter touch conversation, focused more on understanding their market and business model, and less on the exact movement of the data. A large public-sector-adjacent or heavily regulated customer elsewhere may arrive with a long list of non-negotiable requirements. Treating those opportunities as if they belong to the same buying process is a mistake.

However, even where a customer is smaller or less obviously regulated, sovereignty can still matter more than first appears, particularly where that organisation forms part of a wider supply chain or represents an easier route into more sensitive systems and data. Any businesses that accept electronic payments, or sends data over a network, may still be in scope of certain data sovereignty mandates, regardless of their head count.



Small business	Midsize business	Cross-border company	Healthcare/ Finance	Public sector/ Telco
Light-touch sovereignty discussion	More questions around providers and data handling	More legal and operational complexity	Strict regulatory and compliance requirements	Highest scrutiny around control and compliance

THE PENDULUM SWING IS ACCELERATING

Cybersecurity risk, sector regulation, geopolitical tension, and rising executive accountability are all adding momentum to the sovereignty discussion. Frameworks such as DORA and NIS2 are part of that broader shift. They reinforce the expectation that organisations must understand their technology environment properly, manage risk actively, and be able to demonstrate control. Making executives personally responsible adds significant urgency to the topic.

This is not merely a commercial shift, but one the EU itself is willing to back with significant investment and political urgency. In October 2025, the European Commission launched a €180 million sovereign cloud tender[3], which was awarded to four European providers just six months later. There is not only budget behind sovereignty, but clear momentum behind execution. Member states are also making similar investments. The Swiss government alone is investing over €350 million to ensure that its government cloud solutions meet data sovereignty requirements.[4]

In some markets, many smaller organisations still feel comfortable saying that their most sensitive data, such as emails, already sits with large international providers. For them, that can feel like the unavoidable reality of modern IT. However, perceived risk can shift quickly when dependency starts to look more like exposure.

IDC's February 2026 research highlights this nicely, showing that 63 percent of organisations are now more likely to adopt sovereign cloud services specifically because of recent geopolitical events.[5] PWC's November 2025 research showed that 82 percent of organisations were refining their cloud approach in response to geopolitical and/or regulatory change.[6]

Smaller and less data-sensitive organisations are unlikely to lead this shift, but they will tend to follow the path set by larger, more regulated, and more sovereignty-conscious buyers, and their direction of travel is clear.

This impacts partners even more because they are not making short-term choices for individual contracts. They are investing in building relationships with providers who they expect to take to market for years.

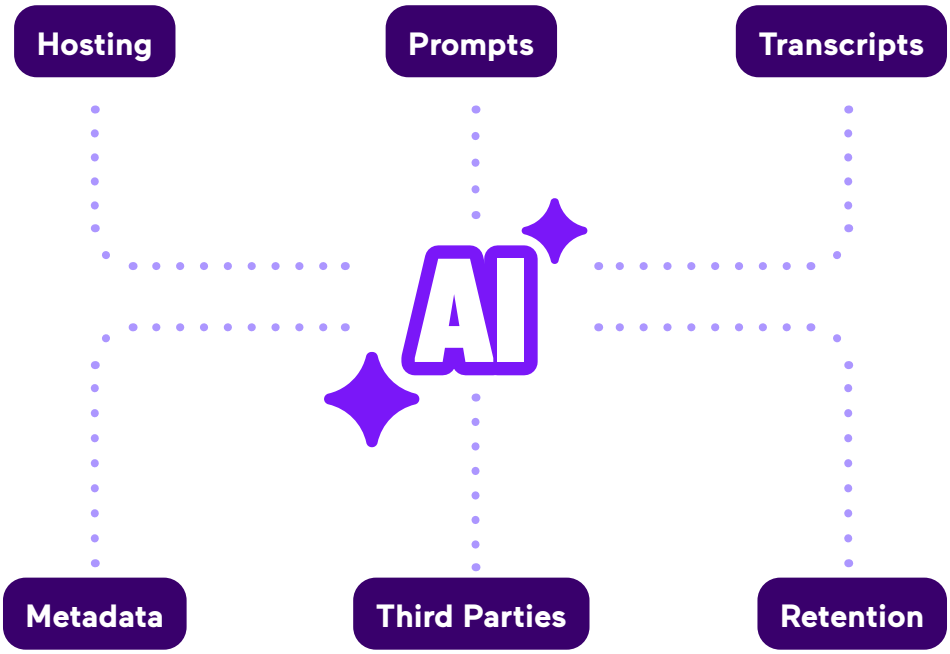
AI HAS MADE THE ISSUE EVEN SHARPER

If sovereignty was already rising in importance, AI has accelerated that trend.

Putting aside cybersecurity concerns, voice AI, transcription, summarisation, copilots, LLM-backed automation, and intelligent routing all create new questions. Which model is being used? Where is it hosted? Is it multi-tenant SaaS or self-hosted? What data is retained? What metadata is created? Which third parties are involved? Can prompts, outputs, recordings, or transcripts cross borders in ways the customer did not expect?

The more intelligence layers a provider adds to a service, the more important it becomes to explain clearly how that service works and what the data path looks like. A solution can appear elegant from a user perspective while hiding significant complexity underneath. Partners need to become more disciplined in how they qualify sovereignty requirements, because customers expect them to have done that due diligence on their behalf.

Innovation is always appealing to a customer, but it is no longer accepted unless the customer can understand, govern, and trust the full operating model around that innovation.



TRACEABILITY IS THE STARTING POINT

Many enterprises still struggle to trace, end to end, where data travels across their stack, which vendors touch it, which services process it, and which jurisdictions may have relevance along the way.

Traceability gives partners something concrete to work with. It turns sovereignty from an abstract concern into a discovery process. Where is the data generated? Where is it stored? Where is it processed? What third-party services are involved? Which systems exchange data with one another? Who has administrative access? Who holds the encryption keys? Which national or sector-specific requirements and regulations apply now, and which may apply over the lifetime of the solution?

These are valuable sales questions, not just compliance questions. The partner that can guide a customer through them adds real value early in the process and is far more likely to avoid painful surprises later.

THE MARKET IS WIDENING NOT REVERSING

Multi-tenant cloud still offers major advantages in scalability, operational simplicity, and pace of innovation. For many customers, it will remain the right answer, especially if it is hosted in a local and compliant fashion.

The range of viable choices is widening. Private cloud, hybrid deployments, in-country managed instances, and other controlled deployment options are regaining relevance because customer requirements are becoming more varied. The debate is not about the model but what it means for the customer in terms of control, compliance, resilience, security, and future flexibility.

Buyers do not care about a deployment model in the abstract. They care about outcomes. Increasingly this also involves not just in country data centres, but geographically proximal data centres with in-country backups.

WHAT THIS MEANS FOR PARTNERS & SERVICE PROVIDERS

Both the opportunity and the risks are clear. Sovereignty is a critical part of the buying process. Customers need help navigating and understanding its complexity.

The winners will be those that combine three things well: deep European understanding at a country level, practical traceability, and deployment flexibility.

That is where 100% European native and owned providers such as Enreach become relevant to the conversation. Buyers increasingly want more than in-country presence, architectural clarity, and deployment flexibility. They also want a provider with deep local knowledge and broader European experience, able to apply lessons from one market to help customers and partners stay ahead in another. Vendors that are market-aware, and not just technically astute, are in a better position to help partners and end users navigate the complexities of sovereignty.

The value for partners is enormous and rapidly expanding. Gartner forecasts that spending on sovereign cloud IaaS alone in Europe will rise from $6.9 billion in 2025, to $12.6 billion in 2026 and $23.1 billion in 2027.[7]

Customers increasingly want providers that can operate at both the European and national levels. They want providers that understand the broader regulatory environment, but also understand that local market realities still matter. They want partners that can explain how services work, not just where the logo sits on a map and they want solutions that can align with real requirements rather than forcing every customer into the same model.

Sovereignty is not a niche issue returning to the market. It is becoming part of a wider reset in how trust is evaluated in enterprise communications and customer engagement. Partners must treat sovereignty as a strategic sales and design issue, not a late-stage compliance question. The more clearly you can map customer requirements, data flows, control points, and local obligations, the more valuable you become.

And in a market where trust is under more scrutiny than ever, that is a powerful place to be.

Sources:

1. Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers
2. IDC's Digital Sovereignty In Europe 2025 Research
3. The European Commission moves forward on cloud sovereignty with a EUR 180 million tender
4. Swiss Government Cloud Project
5. IDC's cost of sovereignty research
6. PWC's November 2025 research on data sovereignty
7. Gartner's Feb 2026 research on sovereign cloud IaaS spending

GET IN TOUCH FOR MORE INFORMATION

For more information about cloud communications and AI solutions built in Europe, for Europe, please reach out. We're happy to answer any questions and put you in contact with our local teams across Europe.

Get in touch on
info@enreach.com

enreach.com

enreach