



# Sovereign Cloud Revived: Strategies for Capturing the New Wave of Growth

In this article we discuss what is fuelling the resurgence of sovereign cloud in Europe and which players are well positioned to take a slice of the growing opportunity

Anna Boyle, Senior Consultant

## What is Sovereign Cloud?

Sovereign cloud refers to cloud infrastructure and services that are designed to process and store data exclusively within a specific jurisdiction.

This concept has gained significant traction in Europe in the past 12 months, where the ascendancy of American hyperscale cloud providers – Google, AWS, Microsoft Azure and Oracle – has become of increasing concern to the EU and its member states' national governments. The European Union's growing emphasis on data sovereignty and cybersecurity is reflected in policies like the Network and Information Systems Directive (NIS2) and the proposed European Cybersecurity Certification Scheme for Cloud Services (EUCCS), which could soon impose mandatory compliance for cloud service providers operating in Europe. These regulations aim to secure the sovereignty of critical digital infrastructure and data.

Regulation isn't the EU's only recourse; it is also providing €1.2 billion in grants to businesses across the edge-cloud value chain to develop European cloud alternatives. This funding project is called IPCEI-CIS or IPCEI Cloud.

## Who is Driving Demand for Sovereign Cloud?

### Governments and other public sector organisations

European governments are avid consumers of the EU sovereign cloud services offered by non-EU providers like Oracle and AWS. These providers have seen the opportunity and are investing vast sums to capture market share – in June, AWS announced its plans to invest €7.8 billion in an AWS European Sovereign Cloud based in Germany with the goal of providing choice “to help public sector organisations meet their evolving sovereignty needs.” The service will be operated by AWS employees who are EU residents and provide cloud services that are operationally independent from existing AWS Regions.

The European Commission has made it clear that it would prefer to use European-owned alternatives. But, no homegrown European cloud providers have the scale or functionality needed to service the requirements of large-scale public-sector organisations. The European Commission's IPCEI Cloud fund is supporting several possible early-stage alternatives including Dynamo Cloud, an intermediary for B2B cloud suppliers, whose goal is to stitch together smaller providers in a seamless way to create a federated edge offering that looks and feels like public cloud. But how successful this will be remains to be seen, particularly as Gaia-X, a European project that set out with similar aims when it was established in 2019, seems to have become a standards body rather than a European cloud champion.

### Businesses with highly commercially sensitive data

While there is some evidence that European governments' position on US cloud providers has softened, it seems that demand for European-owned sovereign cloud has grown among businesses concerned about the security of their sensitive commercial data. In an Amazon-style move, Lidl, needing a sovereign cloud solution to process and store data including pricing calculations and sales patterns, developed a solution to meet its own needs rather than partnering with a hyperscaler. It has since spun the service out into a standalone operating division – Schwarz Digits – which provides very secure, AI-ready, cloud computing services for clients including SAP, FC Bayern Munich and the Port of Hamburg.

There is also a growing cloud repatriation trend, where businesses move workloads back from public cloud to private cloud, colocated or on-premises infrastructure. Security, alongside cost, is one of the key factors driving this trend, a recent STL Partners survey found that 47% of enterprises running workloads in public cloud identified security as the main challenge with their infrastructure.

## Businesses managing critical infrastructure

Companies managing critical infrastructure – such as telecommunications, energy, transport, and finance – have been among the most hesitant to migrate mission-critical workloads to the public cloud. The security risks associated with such a move, are seen as too high, as these could lead to severe economic losses, jeopardise national security, and compromise public safety. However, sovereign cloud solutions offer a way to mitigate these risks by enforcing strict requirements for national data residency and operational independence. France's SecNumCloud certification and Germany's C5 compliance criteria establish rigorous sovereignty and security standards for cloud infrastructure, ensuring that providers of essential services can leverage the cloud while maintaining full control over sensitive data and operations.

## Who is well placed to capture a share of growing sovereign cloud opportunity, and what do they need to do to win?

The hyperscale cloud providers, AWS, Microsoft, Google and Oracle already have sovereign cloud offerings in Europe, but they are being outcompeted by smaller players because some customers and regulators don't find their solutions to be "sovereign" enough. What consumers of cloud are making clear, is that sovereignty is not just about data centre location, it's also about who provides the connectivity to the data centre, and where the company that owns it is headquartered. This, combined with a growing recognition among businesses that they don't always need to pay a premium for the advanced tooling and scalability of public cloud, which is driving cloud repatriation, leaves the door open for challenger sovereign cloud providers to grow their market share with simple, secure and fairly priced propositions:

## Telcos

STL Partners first suggested that there was an opportunity for telcos in sovereign cloud nearly ten years ago. Two things have changed since then, the first is that sovereignty requirements, particularly in Europe, have grown, and the second is that businesses and public sector organisations who have been on cloud transformation journeys for 5+ years are now at the point where they are looking to shift their most precious – secure, mission-critical – workloads away from on-premises solutions to some kind of managed cloud solution.

Telcos are uniquely positioned to capture a slice of the sovereign cloud market because of their distributed geographical footprint and because they are having to develop sovereign cloud services to host their own mission-critical network workloads. There are three ways for telcos to play in sovereign cloud, to create their own, partner with the hyperscalers, or work together to create a sovereign federated edge solution. To date, partnerships with hyperscalers has proved the most popular strategy, and there are several examples of this approach including Orange and Capgemini's joint venture, Bleu, that offers Azure-based IaaS, PaaS, and SaaS that is French-owned and operated.

**Regional data centre players** – Regional data centre operators like nLighten and Equinix have a unique advantage due to their deep-rooted presence in specific geographical areas. These companies have spent years building the physical infrastructure needed to serve local customers, meaning they already have in-country data centres that comply with national sovereignty regulations. Their physical proximity to clients enables them to offer lower latency, enhanced security, and more effective customer support than their global competitors.

**Edge AI solution providers** – Edge AI providers, particularly those focused on federated learning, have a unique value proposition in the sovereign edge-cloud landscape. The decentralised nature of their solutions allows companies to train AI models directly on local devices or servers without transferring sensitive data to a centralised cloud. This approach inherently aligns with the principles of data sovereignty by ensuring that data never leaves its jurisdiction of origin, addressing both security and privacy concerns.

## STL's experience in edge and cloud

STL Partners has undertaken 100+ engagements with clients across the edge and cloud value chain to develop their commercial strategy for edge and cloud computing. We have an industry leading practice, providing market insights. If you are looking for support, or are interested to hear more, check out our [edge computing hub](#), or [book a call with one of the edge team here](#).

*Anna Boyle is a Senior Consultant at STL Partners. She supports clients across the digital infrastructure value chain with growth strategy advice. Anna sits in STL's Edge Computing and Cloud Practice covering topics including the global edge computing market, investment trends and adoption of enterprise and consumer edge computing applications.*

Get in touch with the author to learn more

[anna.boyle@stlpartners.com](mailto:anna.boyle@stlpartners.com)

Or visit STL Partners' Edge Hub

[www.stlpartners.com/edge-computing](http://www.stlpartners.com/edge-computing)