

Europe does not have to choose between moving quickly and building a durable foundation for cloud sovereignty. It can use law now to make cloud services more contestable, public purchasing more strategic and security requirements more concrete—while investing in the infrastructure and skills needed for greater autonomy over time.

The essential distinction is this: sovereignty is not a flag on a data centre. It is the practical ability to keep services running, protect data under European law, understand who controls critical operations, and switch providers without crippling cost. Europe should regulate for those capabilities, not treat European ownership as a shortcut for proving them.

The stakes are substantial. The Commission says the EU relies on non-EU countries for more than 80% of key digital products, services, infrastructure and intellectual property. Its proposed Cloud and AI Development Act (CADA) aims to at least triple EU data-centre capacity within five to seven years, while accelerating deployment and creating a common framework for assessing sovereignty. That is a necessary industrial ambition—but infrastructure takes time to build. The legal and procurement choices Europe makes while it is being built will determine whether the next generation of capacity strengthens European agency or simply deepens dependence.

Make sovereignty measurable

For years, “sovereign cloud” has been an appealing but slippery phrase. Does it mean data sits in Europe? That a European company owns the provider? That European staff operate the service? Or that a third-country government cannot compel access to data or disrupt the technology? These are different questions. A single label can obscure more than it clarifies.

The Commission’s Cloud Sovereignty Framework offers a useful starting point. It assesses services across eight objectives, including legal and jurisdictional control, operations, supply-

chain transparency, technology, security and environmental sustainability. Its Sovereignty Effectiveness Assurance Levels, or SEALs, distinguish degrees of assurance rather than pretending sovereignty is all-or-nothing. In April 2026, the Commission awarded contracts worth up to €180 million over six years to four provider groups, using the framework and requiring at least SEAL-2. One selected partnership uses Google Cloud technology in an environment operated exclusively by EU companies—evidence that control can sometimes be achieved through enforceable operational safeguards, not just by rebuilding every component in Europe.

That is precisely the sort of practical approach public law should reward. CADA should establish a common, risk-based assessment that public authorities can apply consistently across borders. A hospital's patient records, a ministry's classified systems and a municipality's routine website do not present the same risks. Procurement should therefore identify the workload, the threat model and the level of assurance required—then score providers against published criteria. This avoids both extremes: treating every workload as strategically critical, or accepting a provider's "sovereign" marketing claim without evidence.

Use procurement to create demand

Public procurement is one of Europe's fastest available policy levers. Governments are large buyers; when they coordinate demand, they can give suppliers a credible reason to invest, improve services and compete across national borders. CADA proposes a common EU-level procurement framework, while the Commission's 2026 tender demonstrates how measurable sovereignty criteria can be built into a real purchasing decision.

But procurement can also become protectionism by another name. A blanket preference for local ownership, regardless of actual security or resilience, could raise costs, narrow choice and exclude useful technology before alternatives are ready. The Commission's own tender

points toward a more capable standard: it required sovereignty assurance and technical quality, diversified awards across four providers to reduce lock-in, and allowed technology developed outside the EU when strict operational conditions were met.

Europe should scale that approach. Public buyers should use common model clauses, reusable technical assessments and multi-provider awards where feasible. Contracts should specify who holds encryption keys, who can access systems, how incidents are reported, what happens if a supplier or subcontractor is compelled to act, and how workloads can be moved during a crisis. Award criteria should reward meaningful contributions to European research, skills, supply-chain resilience and open technology—but those contributions should be demonstrable, not inferred from a company's passport.

Make exit real

A customer is not sovereign if it cannot leave. Cloud dependence often comes not from where data is stored but from the cost and difficulty of moving applications, data and expertise elsewhere. That makes competition and portability core sovereignty tools, not side issues.

The Data Act, applicable since 12 September 2025, addresses this problem directly. It requires cloud and other data-processing providers to facilitate switching, remove contractual and technical obstacles, and support interoperability. From 12 January 2027, providers must stop charging switching fees, including data-egress charges, although cost-based charges can remain during the transition. The regulation also requires providers to offer routes such as open interfaces and commonly used, machine-readable export formats for relevant services.

The law will matter only if customers can use it. Regulators should monitor whether switching

is genuinely workable, not just contractually promised. Public authorities should test exits before signing long-term agreements: can a workload be transferred, can data be read in a usable format, and can another provider operate the service without an extended outage? The EU should also push for practical interoperability standards and shared migration tools. Portability does not mean every cloud service is identical; it means customers can move without being held hostage by avoidable technical barriers.

Protect data, not just territory

European law already provides important safeguards. GDPR Article 48 says that a judgment or administrative decision from a third country requiring disclosure of personal data may be recognised or enforced only where it is based on an international agreement, without prejudice to other lawful transfer grounds. The Data Act also sets safeguards for foreign-government access to non-personal data held in the EU and points to measures such as encryption, audits and certification.

These protections should be translated into operational controls. Authorities need to know who can decrypt data, whether a provider's parent company can direct local operations, what legal process governs a disclosure request, and whether the customer will be notified where the law permits. Strong encryption, customer-controlled keys, access logging, independent audits and transparent incident reporting can reduce exposure in ways that a data-centre address alone cannot.

Nor should lawmakers imply that any one safeguard eliminates every jurisdictional risk. European and foreign laws can interact in complicated ways. The answer is not to promise perfect insulation, but to assess the risks honestly, limit access technically and contractually, and ensure that decisions about sensitive workloads are made by accountable public authorities.

Build the foundation now

Law cannot conjure a mature European cloud industry overnight. The Commission's estimate that CADA could triple EU data-centre capacity in five to seven years makes the timeline plain. A 2024 study of EU cloud policy also highlights the structural challenge: cloud markets reward scale, investment and broad service ecosystems, while European providers have struggled to match the reach of the largest global suppliers.

That is why Europe should build on what exists while investing in what it lacks. European providers are already partnering with established technology suppliers to deliver managed services under European operational control. One recent example is the Proximus/S3NS partnership in the Commission's tender, which uses Google Cloud technology in an environment operated exclusively by EU companies. Such arrangements are not automatically sovereign; they must satisfy the relevant controls and be independently assessed. But dismissing them simply because the underlying technology is not wholly European would delay useful capacity and weaken local providers' chance to grow.

The same principle applies to open source, research funding, skills and infrastructure. CADA's proposed support for research and development, faster permitting, data-centre deployment and open-source solutions should be judged by whether it creates capabilities that European firms and public institutions can actually use—not just by how many facilities are announced. Europe needs the energy, land, finance, talent and cross-border market access to sustain those services.

Sovereignty is not achieved in a single act of legislation, nor by waiting for a perfect domestic substitute. It is built through rules that reward verifiable control, procurement that creates dependable demand, and markets where customers can leave. Europe can act now—and make those early choices the foundation for deeper autonomy.