



Co-funded by
the European Union

Data Sovereignty as an Operating Model

Why Europe is Re-Architecting Cloud Infrastructure and Talent

Authors: Prof. Gianluca Palermo and Prof. Alessandro Barenghi

Institution: Politecnico di Milano

Data Sovereignty as an Operating Model:

Why Europe is Re-Architecting Cloud Infrastructure and Talent

Authors: Prof. Gianluca Palermo, Prof. Alessandro Barengi

Institution: Politecnico di Milano – Dept. of Electronics, Information and Bioengineering

Data sovereignty is emerging as a defining principle for Europe's digital infrastructure. Beyond data residency, it is shaping how cloud environments are controlled, managed, and made resilient while being kept within a well-defined jurisdiction. However, thinking about infrastructure alone is not enough. Europe's long-term digital sovereignty also depends on its ability to develop the local workforce needed to design, operate, secure, and manage these systems.

In Europe, data sovereignty is no longer just a compliance issue; it is evolving into an operating model for digital infrastructure. This shift is being further encouraged by a regulatory environment that considers more and more control, resilience, and jurisdiction as practical infrastructure issues rather than abstract policy themes. Recent EU initiatives such as the Data Act and DORA reflect this broader evolution, placing a stronger focus on digital control, resilience, and strategic autonomy.

Following this line of thought, sovereignty should not be uniquely identified with simple data residency. Hosting data in Europe is only one part of the issue. The harder question is who operates the environment, who can manage it, where support and identity systems are kept, and under which legal and operational boundaries the platform is kept in working order. The market is already moving in this direction, with all major providers, including Google, Microsoft, and AWS, taking concrete steps to adapt to this evolving framework.

The clearest recent illustration is the AWS European Sovereign Cloud, which became generally available in January 2026. AWS describes it as an independent cloud for Europe,

ACHIEVE project is developed and delivered under European Union's Digital Europe Programme Project no. 101190015



Co-funded by
the European Union

physically and logically separate from other AWS Regions, with its first Region in Brandenburg, Germany. AWS also says day-to-day operations are controlled by personnel who are EU residents located in the EU, with a transition toward exclusive operation by EU citizens located in the EU. Its architecture goes beyond a standard regional deployment: AWS describes a separate partition and dedicated European trust and routing components, designed to operate autonomously within the EU boundary.

What makes this strategically important is that it changes the meaning of cloud design. Sovereignty at this level cannot be simply an add-on label placed on an existing platform; it requires architectural separation, explicit control boundaries, and different resilience patterns. AWS's own design guidance for the European Sovereign Cloud states that the sovereign Region is independent from other AWS Regions, while AWS's architecture guidance on sovereign failover explains that cross-partition continuity introduces additional design requirements because control structures differ between the primary environment and the sovereign target. In practical terms, sovereignty increases the engineering burden since identity management, networking, infrastructure automation, and disaster recovery all have to be designed with jurisdictional separation in mind.

There is an increasing pressure to answer these questions because the demand for AI infrastructure is growing at the same time as the development of sovereignty. The International Energy Agency (IEA) predicts that the global data-center energy consumption will more than double by 2030, with the demand from the EU expected to exceed 100 TWh as AI becomes a major driver of the growth. This is important because sovereign infrastructure cannot rely only on legal desiderata; it also requires local power availability, cooling capacity, and network resilience. Any jurisdiction that wants to keep sensitive computing and data under local control must be able to sustain that control operationally at scale.

A further implication that is often overlooked is that infrastructure sovereignty cannot be sustained without workforce sovereignty. If Europe wants sovereign cloud and data environments operated under local control, it also needs people capable of building, operating, securing, auditing and managing those environments from within Europe. The AWS model highlights this point by explicitly linking operational control to EU-based personnel and moving towards exclusive operation by EU citizens located in the EU. Once sovereignty is defined in this way, talent acquisition becomes part of the control model itself.

This is where Europe's skills gap becomes strategically relevant. According to Eurostat, the EU had 10.3 million ICT specialists in 2024, while 57.5% of enterprises that tried to recruit ICT specialists reported difficulty filling those vacancies. Europe may succeed in defining sovereign requirements for cloud, AI, cybersecurity and critical data infrastructure, but it will struggle to implement them fully if the local talent pool remains insufficient.

This agenda is important not only for regulators and cloud providers, but also for universities and students. The European Commission has established new digital skills academies focusing on areas such as AI, HPC, quantum technologies and virtual worlds, to support Europe's technological sovereignty, competitiveness and resilience. In parallel, the Advanced Digital Skills initiatives by the Commission state directly that Europe needs people to develop, deploy and use cutting-edge digital technologies and infrastructures that support competitiveness and digital sovereignty. For students, educational choices in areas such as cloud engineering, cybersecurity, HPC and AI infrastructures, and data governance are not just about employability. These choices are also becoming an increasingly important part of Europe's capacity to control its own digital future.

Among the European initiatives, we can mention the ACHIEVE project (Advanced Cloud & High-performance computing Education for a Valiant Europe) and its related Master Program in "Cloud and Networking infrastructures and HPC", with a strong focus on innovation and entrepreneurship. The program is part of the EIT Digital Master School and is designed to improve the quality of EU higher education in the domain of IT infrastructures. At Politecnico di Milano, this effort is implemented locally within the MSc in High Performance Computing Engineering, where the curriculum includes dedicated courses on computing infrastructures and contributes to the development of skills relevant to cloud, HPC, and data-center environments.

In this scenario, data sovereignty is best understood as a project combining infrastructure and capability. Europe is trying to determine not only where data should reside, but also to build the legal, technical, operational, and human framework through which digital systems can be trusted to function under European control. Therefore, the most durable sovereign model will not merely localize workloads, but also expertise, accountability, and long-term operating capability. This is why the workforce issue is fundamental to sovereignty.