EuroStack

A Proposed Framework for a “Buy European” Regulation of Strategic Digital Procurement

Briefing Note for EU and Member State Policy Makers

EuroStack Industry Initiative

29 September 2025

EuroStack

1. The Core Problem: A Critical Economic and Security Vulnerability

Europe's escalating **digital dependency on non-EU providers,** particularly from the US and China, has become a **critical economic and security vulnerability**, contributing to an estimated outflow of 360 billion Euros in economic value yearly. This dependency also exposes Europe to supply chain disruptions, data extraction, and the extraterritorial application of foreign laws such as the US FISA and CLOUD Act.

A core pillar of the effort towards lesser dependence and greater resilience in digital must be a **redirection of a portion of public sector demand towards European suppliers**. These must be truly "European" suppliers, for "sovereignty washing" (labelling non-European services as "European") is not going to muscle up Europe's own capabilities and industrial assets.

The EU's current public procurement paradigm—a default "buy from wherever" model—stands in contrast to the established strategic "Buy American" default in the United States and similar policies in other global competitor nations. This systemic flaw in the EU's approach actively hinders the development of a domestic industrial base and perpetuates a cycle of dependency.

The tangible risks of continued inaction are severe and multifaceted:

- **Jurisdictional Risk:** Corporate structures can create a state of **"organized hypocrisy".** A provider can offer "robust" contractual promises to protect all classes of European data, but if its ultimate parent company is non-European, it is legally incapable of resisting disclosure orders from its home government, leaving sensitive information—including citizen health records, industrial R&D, and government data—exposed.

- **Technological Risk:** A narrow focus on data residency is creating **"sovereign prisons"**—systems where data is stored in the EU but is entirely dependent on proprietary, closed-source foreign technology. This leads to vendor lock-in, punitive pricing, lack of resilience, and systemic security vulnerabilities.

- **Economic Risk:** By awarding massive public contracts to non-EU hyperscalers, European public money is funding the R&D and innovation of global competitors. This value extraction starves the European digital ecosystem of the capital and contracts needed to develop competitive, sovereign alternatives.

EuroStack

2. The Solution: A Legally Robust "Sovereign European Technology Provider" Framework

We propose **a new, binding EU Regulation to reverse the current procurement paradigm for strategic digital services** (e.g., cloud, AI). The goal is to establish a clear, legally enforceable preference for genuinely European providers.

This is not a call for a vague "trust" label, but for a rigorous, technical qualification aimed at preventing "sovereignty washing." A "Sovereign European Technology Provider" will be defined by objective, auditable criteria across five distinct dimensions:

I. **Jurisdiction & Governance (Mandatory Prerequisite):** The provider's **ultimate parent entity must be headquartered and legally incorporated in the European Territory** (EU, EEA, EFTA), and be free from decisive non-EU control.

II. **Technical Sovereignty:** The service **must be built on open standards and predominantly open-source software** to prevent vendor lock-in, guarantee interoperability, and ensure operational reversibility.

III. **Operational Sovereignty:** The entire service delivery chain— from data centers to the operational control plane and privileged personnel—must be **located and managed exclusively from within the European Territory.**

IV. **Data Sovereignty:** All customer data, including metadata and backups, must **reside exclusively within the EU.** Verifiable technical measures must be in place to make it cryptographically impossible for the provider to access unencrypted customer data.

V. **Economic Sovereignty:** The provider must be a **net contributor to the European economy,** with a majority of its global R&D for the core technology located within Europe.

3. Legal Foundation: The “Essential Security Interests” Exception

A “Buy European” mandate should not be seen to conflict with the WTO’s Government Procurement Agreement (GPA), which mandates non-discrimination. The legal basis for this is found within the GPA itself: **Article III – Security and General Exceptions.** This article, mirrored in Article 346 of the TFEU, allows nations to take measures necessary to protect “essential security interests.”

Public digital infrastructure and its sensitive data are indispensable for national security. Exposure to the extraterritorial reach of foreign laws is an unacceptable risk. Framing this as a security requirement transforms the mandate from prohibited economic discrimination into a legitimate sovereign action, fully compatible with the GPA.

4. The Instrument: A Regulation for Speed and Uniformity

To be effective, the criteria for a “Sovereign European Technology Provider” must be applied with speed and uniformity across the Single Market. For these reasons, a Regulation is the only viable legal instrument:

- **A Directive is insufficient:** A typical two-year transposition period would cause unacceptable delays. Furthermore, 27 different national interpretations would be subject to local lobbying and political compromise, creating loopholes and a fragmented market.
- **“Soft law” is ineffective:** Non-binding guidelines are routinely ignored by contracting authorities who are bound by existing hard laws. This would guarantee inaction.
- **A Regulation provides the necessary speed of implementation and uniformity of application,** creating a predictable, harmonized European market for sovereign digital services and preventing “sovereignty shopping”by non-EU providers.

5. Practical Application in Public Procurement

The framework is designed to be translated directly into the established, legally recognized structure of public tenders, using a clear two-step process:

- **Step 1 (Pass/Fail Gate): The Jurisdictional Prerequisite as a Selection Criterion.**

In line with the Public Procurement Directive (2014/24/EU), the criteria for **Jurisdiction & Governance** will be a mandatory selection criterion. Bidders will be required to provide verifiable evidence (e.g., corporate registry documents, declaration of Ultimate Beneficial Ownership) of their ultimate accountability to EU law. Any bidder failing to meet this prerequisite is deemed legally incapable of delivering a sovereign service and is **immediately disqualified** from the tender process.

- **Step 2 (Qualitative Scoring): Other Dimensions as Technical & Award Criteria.**

For bidders who pass the jurisdictional gate, the criteria within **Technical, Operational, Data, and Economic Sovereignty** are used to evaluate the quality of the service being offered. Contracting authorities, guided by proportionality, will define mandatory minimums (technical specifications) and score the remaining criteria to differentiate offers. This allows the selection of the bid that offers the highest level of sovereignty and strategic value to Europe.

6. Formal Request and Call to Action

The risks of inaction are growing. The necessary legal analysis has been done, and the technical criteria have been defined. We formally call upon the **European Commission**—specifically EVP Stéphane Séjourné, EVP Henna Virkkunen, DG Connect, DG IT, and DG Grow—and the **relevant Ministries of the Member States** to:

1. **Adopt** this comprehensive framework as the definitive standard for defining a “Sovereign European Technology Provider.”

2. **Initiate immediately** the legislative process for a new EU Regulation based on the legal and technical foundation outlined herein.

3. **Ensure** this framework serves as the binding technical basis for the forthcoming legislative act on cloud and AI procurement.