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

EuroStack Industry Initiative[1]

EuroStack

29 September 2025

Contents

[1] This document has been authored by multiple individual supporters of the *EuroStack Industry Initiative,* and has been subject to legal review from procurement specialists. The EuroStack Industry Initiative is a non-lobby group of unpaid volunteers, including industry and tech experts. **As for all our previous documents, this contribution does not purport to represent the views of all signatories to our original Open Letter, nor should it be understood as a proposal undersigned by any of them individually or collectively.** It is intended to make a contribution to the necessary adoption of “Buy European” rules and the principles are widely shared among supporters.

1. Executive Summary

Europe's escalating digital dependency on non-EU providers (US and China) has become a critical economic and security vulnerability (as vocally recognized also by Mario Draghi in his recent Report on Competitiveness – One Year On). Foreign states are increasingly using this dependency as geopolitical leverage, exposing the EU to supply chain disruptions, data extraction, and the extraterritorial application of foreign laws. Europe's predicament is **perpetuated by the EU's own public procurement paradigm, a default "buy from wherever" model that stands in contrast for instance to the "Buy American" default that actively builds industrial capacity in the United States – and the plain obligation to use only local suppliers in China and elsewhere.**

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.

This document outlines a comprehensive proposal for a framework to set a **new, binding EU Regulation** to reverse our "upside down" paradigm for strategic procurement of digital services. We need a new Regulation to establish a **clear, legally enforceable preference for genuinely European providers.** We develop a clear definition of what "European" should mean. We explain that the legal foundation for this mandate must be the **"essential security interests"** exception**,** a provision within the WTO's Government Procurement Agreement (GPA) and other trade deals, which makes this muscular, pro-European industrial strategy fully compatible with our international obligations.

To prevent circumvention and "sovereignty washing" (e.g., via the "Irish subsidiary" loophole), we propose a multi-dimensional framework to define a **"Sovereign European Provider"**. This is not a vague label or a moral judgment on "trustworthiness"; it is a rigorous, technical test of substantive control and operational autonomy. It provides objective, auditable criteria to ensure a provider is structurally immune to non-EU control and legal coercion.

Our framework is built on three clear and pragmatic principles:

1. **IT-Only Focus:** The scope is strictly limited to strategic digital technologies (cloud, AI, etc.) where the national security argument is strongest. This ensures a solid legal footing and avoids a broader debate that could dilute and delay the entire initiative.
2. **Control is Everything:** The definition of "European" is based on the non-negotiable reality of ultimate corporate control. This means will require an assessment of the ultimate parent entity's headquarters, majority ownership, and verifiable insulation from non-EU laws.
3. **Beyond Data—Technological Autonomy:** The framework is explicitly designed to ensure Europe avoids "sovereign prisons"—secure systems where our data is locked into proprietary technology. It mandates openness, interoperability, and operational reversibility to guarantee Europe has the freedom to innovate and the ability to switch providers, ensuring we "stay by choice, not by lock-in".

2. The Strategic Imperative: Reversing the EU Procurement Paradigm

To understand why a new Regulation is not just an option but a necessity, we must first identify and acknowledge the fundamental, systemic flaw in the European Union's current approach to public procurement. Our model, designed for an era of open markets and good- faith competition, has become a strategic vulnerability in a world of geopolitical rivalry.

2.1. The Systemic Flaw: "Buy American" vs. "Buy from Wherever"

There is a profound philosophical and strategic divide between how the United States and the European Union view public procurement.

- **The US Model: "Buy American" by Default.** The United States treats public procurement as a primary instrument of its industrial and national security strategy. The Buy American Act establishes a clear and unambiguous **default position**: public money should be spent on American goods and services. While exceptions exist to comply with international trade agreements, the foundational principle is to nurture a protected, predictable, and resilient domestic market. This approach has been instrumental in creating and sustaining global technology champions.

- **The EU Model: "Buy from Wherever" by Default.** The European Union, by contrast, has designed its procurement paradigm on the principles of the Single Market: absolute non-discrimination and equal treatment, as enshrined in the Treaty on the Functioning of the European Union (TFEU). While this is a powerful tool for economic integration *within* the EU, it becomes a critical weakness when applied globally without any guarantee of reciprocity. Our legal default is "open to all". Consequently, any attempt to favor a European provider over a non-European provider with whose home country an international trade agreement exists, becomes a complex, legally fraught exception that must be painstakingly justified, case by case.

We are arguing for a reversal of this logic. For strategic technologies, the EU must adopt the same pragmatic approach as its global competitors. **The default assumption must become "procure sovereign" with exceptions made only when no viable European alternative exists.**

2.2. The Threat Model: The Tangible Costs of Inaction

Failing to reverse this paradigm exposes the European public sector (and ultimately our businesses and citizens) to a range of severe and escalating risks. **The status quo should not be perceived as a neutral position, but as an active acceptance of vulnerabilities that our competitors would never tolerate.**

- **Jurisdictional Risk: The Erosion of Our Legal Order**

  The most direct threat is our exposure to the extraterritorial reach of foreign laws, most notably the US CLOUD Act and FISA 702. A non-EU technology provider, even when operating through a legally incorporated EU subsidiary (the "Irish Subsidiary" loophole), remains ultimately bound by the laws of its home country. This creates a state of **'organized hypocrisy'**: a provider can offer contractual promises of GDPR compliance while being legally obligated by its own government to disclose European public data. This means **our public data—from citizen health records to tax information—is not truly sovereign. It is, by definition, subject to the legal and political decisions of a foreign power.**

- **Technological Risk: The "Sovereign Prison"**

  A narrow focus on data **residency** alone creates a dangerous illusion of security. We risk building a **"sovereign prison"** -- a system where our data is securely stored within EU borders but is completely dependent on proprietary, closed-source foreign technology. This technological dependency creates severe risks, including vendor lock-in, punitive pricing models (especially for data egress), an inability to audit source code for vulnerabilities, and the existential threat of a provider discontinuing a service or being acquired. In this scenario, Europe has protection but no **agency**; data security but no **technological autonomy**.

- **Economic Risk: The Extraction of European Value**

  By awarding massive public contracts to non-EU hyperscalers (directly or indirectly through “sovereignty washing” European entities), we are actively funding the innovation of our global competitors with our own public money. The dominant business model involves winning European contracts, repatriating the profits, and conducting the vast majority of high-value Research & Development and IP creation outside of Europe. The EU is relegated to the role of a profitable consumer market and a location for sales offices, not a hub of core technological creation. This **value extraction** starves our own digital ecosystem of the capital, contracts, and scale needed to develop competitive, sovereign alternatives.

3. The Framework: A Multi-Dimensional Definition of a "Sovereign European Provider"

To create a legally enforceable "Buy European" mandate, we must first establish a definition of "European" that is precise, objective, and immune to the "sovereignty washing" that currently plagues the market. This proposed framework provides that definition.

3.1. Guiding Principle: Technical Assessment, Not a "Trust" Label

First, we must be clear about what this framework is and what it is not. Misleading marketing terms like "Trusted Provider" must be abandoned. This is not a moral judgment on a company's character or a subjective assessment of its trustworthiness. We do not care, in this context, if a provider is "dodgy"; we care if it is structurally and verifiably European.

Our framework defines a **"Sovereign European Provider"** based on a set of objective, auditable criteria. It is a technical qualification, not a badge of honor.

A provider either meets the specific, verifiable standards of corporate structure, operational control, and legal insulation, or it does not. This approach is essential to create a legally robust standard that can withstand challenges from non-EU competitors and provide absolute clarity to public procurement authorities.

3.2. The Five Dimensions of Sovereignty

A one-dimensional definition focusing only on data location is dangerously insufficient and leads directly to the "sovereign prison". True sovereignty requires a holistic view that combines passive protection with the active freedom to act and innovate. Our framework is therefore built upon five distinct, comprehensive dimensions:

I. Jurisdiction & Governance: Ultimate accountability to EU law

This dimension answers the question: **"To which legal and political system is the provider ultimately accountable?"** It serves as the non-negotiable legal bedrock of sovereignty and is designed to definitively close the "Irish subsidiary" loophole. It ensures that a provider's promises of compliance are not rendered meaningless by conflicting legal obligations to a non-EU state.

- **EU Domicile and Governance:** It is not enough for a provider to have a local branch in Europe. Its **Ultimate Parent Entity** - the top of its corporate control chain - must be legally incorporated and have its headquarters within the European Territory (EU, EEA, EFTA).

- **European Control and Ownership:** Formal domicile is insufficient if a non-EU entity can exercise decisive influence. A sovereign provider must be free from non-EU control, both *de jure* (formally, with a majority of ultimate voting rights held by Europeans) and *de facto* (substantively, with no non-EU entity holding a blocking minority stake or other mechanisms of coercive influence).

- **Jurisdictional Supremacy:**
  The provider must be structurally and legally insulated from the extraterritorial reach of non-EU laws (e.g., US CLOUD Act, FISA 702). This includes being free from non-EU export controls or restrictive IP licenses on its core technology that could be used as a geopolitical lever to disrupt service.

II. Technical Sovereignty: Freedom from technological lock-in

This dimension answers the question: **"Does the technology empower or encage the customer?"** It is the essential antidote to the "sovereign prison", ensuring that Europe's digital future is not dependent on proprietary, opaque technologies. It guarantees technological autonomy.

- **Interoperability and Portability:** The service must be built on **open standards** and predominantly use **Open Source Software** for its core components. This guarantees data and workload portability, preventing vendor lock-in and allowing customers to switch providers freely - ensuring they "stay by choice".**Architectural Transparency:** The service cannot be an unauditable "black box". The source code for core technology must be available for inspection by the customer or a trusted European third party. This replaces blind trust with verifiable proof, mitigating the risk of hidden vulnerabilities or backdoors.

- **Operational Reversibility:** The service must be designed and documented in a way that allows a competent third party to redeploy and operate it in the event of provider failure or contract termination.

This transforms a rented service into a resilient, transferable industrial capability, decoupling a customer's mission-critical operations from a single provider's viability.

III. Operational Sovereignty: Control over the entire service delivery chain

This dimension answers the question: **"Who has control over the operational environment?"** It closes major loopholes where data can reside in the EU but be managed from the outside, ensuring the entire operational chain is under European control.

- **EU Infrastructure and Control Plane:** The entire physical infrastructure (datacenters, networks) and, critically, the **operational control plane** used to manage and orchestrate the service must be located and operated from within the European Territory.

- **Exclusive European Personnel:** All personnel with privileged access to infrastructure or customer data must be residents of the European Territory, employed by a European entity, and physically perform all their duties from within the EU. This creates a "human firewall", ensuring no system administrator can be legally compelled by a non-EU authority to access data or alter the system.

- **Supply Chain Resilience:** The provider must have a documented and auditable strategy to mitigate dependencies on non-European hardware and critical software, ensuring service continuity in the face of geopolitical sanctions or supply disruptions.

IV. Data Sovereignty: Verifiable protection of all data

This dimension answers the question: **"Is the data verifiably protected, both legally and technically?"** It moves beyond contractual promises to demand tangible proof of data protection.

- **Exclusive EU Data Residency:** This is a bright-line rule. All customer data - including all associated metadata, backups, and logs - must be stored and processed exclusively within the European Territory. No data, in any form, may be transferred or made accessible outside this territory.

- **Technical Data Access Protection:** Legal promises are insufficient. The service must provide verifiable technical measures, such as **confidential computing or customer-exclusive key management**, to make it cryptographically impossible for any party, including the provider itself, to access unencrypted customer data.

- **Legal Data Access Guarantees:** The provider must be contractually obligated to legally challenge any non-European governmental request for data disclosure and to notify the customer of such requests. This ensures the provider acts as an advocate for its customer's rights.

V. Economic Sovereignty: Net contribution to the European economy

This dimension answers the question: **"Is the provider a net contributor to, or an extractor of value from, the European economy?"** It ensures that public money is used to build a resilient and competitive European industrial base, not to fund the R&D of our global competitors.

- **European Value Creation:** The majority of the provider's global R&D expenditure and personnel for the core technology must be located within the European Territory. This ensures that the intellectual property and high-value skills that drive the digital economy are developed and retained in Europe.
- **Fair and Transparent Business Model:** The provider's business model must be free from punitive lock-in tactics, such as exorbitant data egress fees or tied-selling, that prevent the emergence of a competitive European market.
- **Commitment to the European Ecosystem:** The provider must demonstrably strengthen the European digital ecosystem through active partnerships with European SMEs, meaningful contributions to Open Source projects, and investment in skills development.

3.3. A Clear Hierarchy for Practical Application

The five dimensions of sovereignty are not all equivalent, nor should they be applied as a simple, flat checklist. To be effective in a real-world public procurement process, they must be structured in a logical hierarchy that reflects their dependencies. This pyramid provides a clear, step-by-step methodology for procurement authorities, ensuring a rigorous evaluation process that is both legally defensible and immune to "sovereignty washing".

Level 1 (Mandatory Prerequisite / Pass-Fail): Jurisdiction & Governance

This dimension is the absolute bedrock of the entire framework. It is the first, non-negotiable filter through which any potential provider must pass.

The Logic: A provider's technical capabilities and operational promises are meaningless if the provider itself is ultimately subject to the laws and coercive influence of a non-EU government. Guarantees of data protection, operational control, and even technological openness are built on sand if they can be nullified by a legal order from a foreign state (e.g., a US Executive Order). Therefore, a provider's fundamental legal and corporate structure must be verifiably European *before* any other aspect of its service is considered.

- **Application in Procurement:** This dimension functions as a **pass/fail gate**. At the very beginning of the evaluation process, the contracting authority will conduct due diligence on the provider's compliance with all criteria within the Jurisdiction & Governance dimension (Ultimate Parent Entity in the EU, freedom from non-EU control, etc.).
  - If the provider **fails** to meet these mandatory prerequisites, their bid is **disqualified and excluded from any further consideration.**
  - If the provider **passes**, they are eligible to proceed to the next stage of evaluation.

This binary approach provides absolute clarity and prevents providers who are not structurally sovereign from using their technical or marketing strengths to obscure their fundamental lack of jurisdictional integrity.

Level 2 (Core Guarantees): Technical, Operational, and Data Sovereignty

For providers who have passed the Level 1 gate, these three dimensions represent the heart of the sovereign service offering. They are the essential, active capabilities that provide verifiable proof of a service's day-to-day sovereignty.

The Logic: These dimensions are interlocking and mutually reinforcing. They represent the complete set of active controls over a digital service:

- **Data Sovereignty** protects the asset itself (the data).
- **Operational Sovereignty** protects the environment (the infrastructure, processes, and people).
- **Technical Sovereignty** protects the future (the freedom to migrate, innovate, and avoid lock-in).
  Together, they provide the tangible assurance that a service is not just legally European on paper, but is operated and managed in a way that delivers true sovereignty in practice.

Application in Procurement: These dimensions form the basis of the **core technical and operational evaluation**. Based on the sensitivity and criticality of the specific use case (the principle of proportionality), the contracting authority will define the *minimum acceptable* assurance levels for each of these three dimensions. For Example:

- A contract for **national security data** would require the highest possible rating across all three Core Guarantees. No compromises would be acceptable.
- A contract for **citizen health records** would require the highest ratings on Data and Operational Sovereignty, with a high rating on Technical Sovereignty being critical to ensure long-term data accessibility.
- Any provider failing to meet these pre-defined minimums would be deemed non-compliant.

Level 3 (Key Differentiator): Economic Sovereignty

This dimension is used to evaluate providers who have successfully passed the Level 1 prerequisite and have met the minimum requirements for the Level 2 Core Guarantees. It distinguishes a mere supplier from a true strategic partner committed to Europe's long-term success.

- **The Logic:** While a provider's contribution to the local economy is secondary to its ability to deliver a secure and sovereign service, it is a critical factor in building a resilient European industrial base. This dimension measures a provider's maturity, its commitment to fair competition, and its investment in the European digital ecosystem.
- **Application in Procurement:** This dimension functions as a **powerful differentiator** in a competitive tender. In a scenario where two or more providers are fully qualified at Levels 1 and 2, their performance on the Economic Sovereignty criteria becomes decisive. The contracting authority can use these criteria in the final award stage to select the provider that offers the greatest strategic value to Europe. The provider who scores higher on European R&D investment, fair business practices, and ecosystem contributions would be awarded the contract. This creates a powerful incentive for providers to be not just *operating* in Europe, but to be actively *investing* and *contributing* to its sovereign digital future.

4. The Legal Pathway to Implementation

A robust framework is only as good as its legal enforceability. The strategy outlined in this document is designed to be implemented as binding law, fully compatible with the European Union's existing international commitments.

4.1. Legal Foundation: The "Essential Security Interests" Exception

A challenge to any "Buy European" mandate will be perceived to be its apparent conflict with international trade law, most notably the World Trade Organization's Government Procurement Agreement (GPA). The GPA, to which the EU is a signatory, is built on a principle of non-discrimination, obligating member states to provide fair and open market access to companies from other signatory nations. A simplistic, protectionist "Europeans Only" rule would violate this agreement and lead to legal challenges and trade disputes.

The legal strategy should be therefore predicated on a powerful, explicit, and legitimate provision within the GPA itself: **Article III – Security and General Exceptions.**

This article states that nothing in the agreement shall be construed to prevent any party from:

> *"...taking any action or not disclosing any information that it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes."*

This is a sovereign right that all signatories, including the United States, have retained. This right is also explicitly reflected in the EU's own foundational law, particularly Article 346 TFEU, which affirms the right of Member States to take such measures as they consider necessary for the protection of the essential interests of their security. Europe's legal pathway needs to formally and justifiably invoke this right for the procurement of strategic digital technologies, particularly given the new geopolitical realities.

The Argument: The position should be that the public sector's digital infrastructure and the vast repositories of sensitive government and citizen data it contains are **"indispensable for national security".** As detailed in our Threat Model (Part 2.2), the exposure of this infrastructure to the extraterritorial reach of foreign laws, potential supply chain disruptions, and technological dependencies constitutes a direct and unacceptable risk to the essential security interests of the European Union and its Member States. "Digital Sovereignty" is not an economic preference; it is a modern component of national security.

Compatibility: By framing this mandate as a security requirement, it is transformed from a prohibited act of economic discrimination into a legitimate and legally sound sovereign action. This approach has several key advantages:

- **It is WTO-Compatible:** It uses an explicit mechanism provided within the GPA, mirroring the same legal logic used by other nations to protect their own strategic industries.
- **It is Targeted and Proportional:** By limiting the scope strictly to strategic IT, we ensure the measure is proportional to the threat, strengthening its legal defensibility. We are not closing our entire procurement market, only securing the digital assets that are critical to the functioning and security of the state.
- **It Provides a Defensible Rationale:** It allows us to implement the stringent, multidimensional criteria outlined in Part 3 not as arbitrary barriers to entry, but as **necessary and objective security requirements.** A procurement authority can already now legally require a provider to be free from non-EU control if that control represents a verifiable jurisdictional security risk.

Note: the argument here is that the “national security exception” in the GPA can and should be used to address general objections to “Buy European” based on trade/procurement law. We are not arguing that the EU can and should use the “national security interest” to harmonise all member states’ procurement preferences and disallow them from pursuing their core national interest (e.g. to forbid – say – Poland from buying South Korean tanks and American missiles if Poland believes these are essential for its national security interests).

The point is rather that in our new era of geopolitical realism, the national security exception in the GPA can and should be used to overcome objections based on international contracts like the GPA.

This security-based foundation is the legal cornerstone that makes the entire framework possible. It gives the EU the authority to act decisively to protect its digital sovereignty while fully respecting its international legal obligations.

4.2. The Instrument: A Regulation

The choice of legal instrument will determine whether this framework becomes an effective tool of industrial strategy or an irrelevant policy paper. To achieve the objective, the criteria for a "Sovereign European Provider" must be applied with speed, uniformity, and legal force across the entire Single Market. For these reasons, a Regulation is most realistic path forward. "Soft law" recommendations are ineffective, and a Directive is insufficient.

Why a Regulation? Speed and Uniformity

A Regulation, **as defined in Article 288 TFEU**, is a law that is **directly applicable** in all EU Member States the moment it enters into force. This provides two critical advantages:

1. **Speed of Implementation:** In the fast-moving digital sector, a multi-year delay is a strategic failure. A Regulation bypasses the lengthy national transposition process, ensuring that the new procurement rules are implemented simultaneously across the Union. This allows us to respond to the urgent security and economic threats without delay.
2. **Uniformity of Application:** This is the most crucial benefit. A Regulation creates a single, harmonized set of rules for the entire Single Market. It prevents the fragmentation that would inevitably arise from 27 different national interpretations. It ensures that a provider deemed "sovereign" in Germany meets the exact same high standard as one in Poland or Spain. This creates a predictable and unified European market for sovereign digital services and prevents non-EU providers from "sovereignty shopping" by targeting Member States with weaker implementations.

Why a Directive is Insufficient: A Recipe for Delay and Fragmentation

A Directive sets a goal that all EU countries must achieve, but it is up to each individual country to devise and pass its own laws to meet that goal (a process called "transposition"). While suitable for some policy areas, this instrument has fatal flaws for our purpose:

- **Built-in Delay:** The transposition period, typically two years, would create a significant and unacceptable lag between the political decision and its practical effect on the ground.
- **The Certainty of Inconsistency:** During the national transposition process, the clear, robust criteria outlined in our framework would be subject to national lobbying, political compromises, and differing legal traditions. The definition of "European control" or "technological autonomy" could be weakened in some Member States, creating loopholes that non-EU providers would immediately exploit. This would shatter the concept of a single standard, creating a fragmented and ineffective policy. A Directive would give us 27 different, weaker versions of one good idea.

Why Guidelines are Ineffective: A Guarantee of Inaction

So-called "soft law" instruments, such as Communications or Guidelines from the Commission, are not legally binding. They are recommendations, and as such, they are wholly inadequate for this task.

- **No Legal Force:** A contracting authority in a Member State is legally bound by their national procurement laws and the existing EU Directives. They cannot legally favor a European provider based on a non-binding guideline if it contradicts these hard laws. Doing so would expose them and their authority to legal challenges from any rejected non-EU bidder.
- **A History of Being Ignored:** Faced with this legal risk, officials will invariably follow the letter of the binding law and ignore the recommendation. The Commission has published numerous guidelines on strategic procurement in the past; they are almost universally unknown, unused, and unapplied. Relying on "soft law" is a proven recipe for inaction and would ensure the status quo remains unchanged.

To succeed, we need legal certainty and a level playing field. A Regulation can provide both.

4.3. Application to Public Procurement: Translating the Framework into Legally Sound Tenders

The five-dimension framework is designed not as an academic exercise, but as a practical tool for immediate use. Its strength lies in its ability to be translated directly into the established, legally recognized structure of a public tender document. This is achieved by mapping the sovereignty dimensions onto two distinct and standard components of procurement law: **selection criteria** (which assess the bidder) and **technical specifications/award criteria** (which assess the offer).

This two-step process provides a clear, defensible, and rigorous methodology for any public authority.

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

The criteria within **Dimension I: Jurisdiction & Governance** will be formulated as mandatory *selection criteria*, in line with Article 58 of the Public Procurement Directive (2014/24/EU).

- **What this means:** Selection criteria are used in public procurement to assess the fundamental eligibility and capacity of a bidder to perform the contract. They are about the *company* itself - its legal, financial, and professional standing. They are not an evaluation of the specific service being offered.
- **Why this is the correct legal approach:** Our definition of a "Sovereign European Provider" posits that a company substantively controlled by a non-EU entity is, by its very nature, legally incapable of guaranteeing a sovereign service. Its jurisdictional status is a fundamental question of its capacity to deliver on the core security requirements of the contract. Framing this as a selection criterion is therefore the appropriate and legally sound mechanism.
- **How it works in practice:** A public tender will require all bidders to provide verifiable evidence (e.g., official corporate registry documents for the entire provider group, a formal declaration of Ultimate Beneficial Ownership, and a signed legal attestation of freedom from non-EU jurisdictional control). The contracting authority will review this evidence as the first step.
    - Any bidder that fails to demonstrate full compliance with the Jurisdiction & Governance criteria is deemed **ineligible to participate**.
    - Their bid is **rejected and excluded** from the process before any technical or financial evaluation even begins.

This creates a clean, binary, and legally defensible pass/fail gate that filters out any provider who is not structurally sovereign from the outset.

Step 2: Evaluating the Sovereign Service via Technical Specifications and Award Criteria (Proportionality in Action)

For bidders who have passed the jurisdictional gate, the criteria within **Dimensions II-V** are used to evaluate the quality and compliance of the *service being offered*. This is done using a combination of mandatory minimums and qualitative scoring.

- **Technical Specifications (The Mandatory Baseline):**

  The contracting authority, guided by the principle of proportionality, will define the nonnegotiable minimum requirements for the specific use case. These are the "must-haves".

  - **Example:** For a tender involving sensitive citizen data, the authority would designate "Criterion 4.1: Exclusive EU Data Residency" (including all metadata) as a mandatory **technical specification**.
  - **Consequence:** Any bid whose proposed service does not meet this mandatory baseline is deemed technically non-compliant and is rejected.

- **Award Criteria (The Quality Score):**

  For all bids that are compliant with the technical specifications, the remaining criteria are used to score the quality of the offer. This is where the nuanced, risk-based evaluation occurs and where the multi-level assurance model becomes a powerful tool.

  - **Example 1 (Technical Sovereignty):** A provider achieving "Level 2 (High Assurance)" on "Criterion 2.1: Use of Open Source Software" by building its core service on building OSI-approved licenses will receive a higher score than a provider at "Level 1 (Partial Assurance)" that uses proprietary APIs.
  - **Example 2 (Economic Sovereignty):** In the final scoring, a provider demonstrating that >50% of its global R&D is in Europe ("Criterion 5.1") will be awarded more points than a competitor that only meets a lower threshold.
  - **Consequence:** This approach allows the contracting authority to differentiate between compliant bids and select the one that offers the highest level of sovereignty. It creates a powerful market incentive for providers to go beyond the minimum requirements and to compete on the quality of their sovereignty offerings.

By using this standard two-step procurement methodology, we embed our sovereignty framework into a legally familiar and robust process. It gives public officials a clear, step-by-step guide to move from abstract principles to a concrete, defensible call for tender procedure or contract awarding.

5: Conclusion & Next Steps

Recap of the Proposal

The framework outlined in this document is a complete, end-to-end strategy to address one of the most critical challenges facing the European Union. It offers a **focused, pragmatic, and legally robust** plan to build Europe's sovereign digital industrial base using the powerful and underutilized lever of strategic public procurement.

We have moved beyond abstract principles to provide a concrete solution. This framework successfully reverses the EU's flawed "buy from wherever" procurement paradigm by establishing a legally sound pathway, predicated on the "essential security interests" exception of our international trade agreements. It offers a clear, objective, and multidimensional definition of a "Sovereign European Provider" that is immune to circumvention and "sovereignty washing". Crucially, it provides a practical implementation model that maps these criteria directly onto the standard, legally recognized procedures of public tender documents.

Formal Request and Call to Action

The time for abstract discussion is over. The risks of inaction are clear, growing, and documented. We have moved beyond identifying the problem to engineering a complete, legally robust, and actionable solution. A comprehensive, ready-made answer to the call for a definition of sovereignty is now on the table.

We need to move from analysis to action.

We formally call upon the **European Commission**, specifically **EVP Stephane Séjourné, EVP Henna Virkkunen, DG Connect 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 Provider" in the context of strategic public procurement for all digital technologies, including cloud and AI.
2. **Initiate immediately the legislative process for a new EU Regulation** based on the legal and technical foundation laid out in this document. This Regulation must reverse the **current** procurement paradigm by establishing a clear, legally enforceable preference for providers who meet these sovereignty criteria.
3. **Ensure this framework serves as the binding technical basis** for the forthcoming legislative act on cloud and AI procurement, fulfilling the explicit political mandate set forth by the European Parliament.

This framework provides the blueprint to reclaim our digital autonomy, foster a competitive European ecosystem, and ensure our public sector is built upon a foundation of sovereign technology. The necessary legal analysis has been done, the technical criteria have been defined, and the political will is present.

The time to build is now.

Annex: The Five Dimensions of a Sovereign European Provider – Detailed Criteria

This annex provides the detailed, auditable criteria for the five dimensions of sovereignty that form the core of this framework. These definitions are designed to be objective and verifiable, providing a clear methodology for public procurement authorities and a transparent standard for the market. The objective is to replace vague marketing labels with a rigorous, technical qualification for a "Sovereign European Provider". This is necessary because simpler, existing legal definitions of origin, such as that found in Article 3 of the EU's International Procurement Instrument (IPI) Regulation (EU) 2022/1031, are insufficient to prevent the circumvention this framework is designed to stop.

The criteria are structured according to the hierarchy outlined in Part 3 of this document: a mandatory prerequisite, three core guarantees, and a key differentiator. They are intended to form the substantive basis for a new EU Regulation on strategic digital procurement.

I. JURISDICTION & GOVERNANCE (Mandatory Prerequisite / Pass-Fail)

Core Question: *To which legal and political system is the provider ultimately accountable?* This dimension ensures a provider is structurally and legally European, making it immune to non-EU legal coercion. A provider's failure to meet any criterion in this dimension results in immediate disqualification.

Criterion 1.1: EU Domicile and Governance

- **Objective:** To verify that the provider's entire chain of control is legally based in the European Territory.
- **Core Requirement:** The provider and its entire chain of parent entities, up to and including the **Ultimate Parent Entity**, must be legally incorporated and maintain their statutory headquarters within the European Territory (EU, EEA, or EFTA).
- **Justification & Threat Model:** This is the absolute foundation for the rule of law in the digital sphere. The central threat is a direct and irreconcilable conflict of laws (e.g., the US CLOUD Act vs. GDPR). Without this criterion, non-EU providers operate in a state of ”organized hypocrisy”', offering contractual promises of compliance while being legally bound to obey their own government's mandates. This criterion ensures the provider is **structurally immune** to such conflicts, making European law the sole and ultimate authority.

Criterion 1.2: European Control and Ownership

- **Objective:** To verify that decisive influence over the provider is held by European entities, free from non-European control.
- **Core Requirement:** The provider must be free from non-European control, both *de jure* (formal) and *de facto* (substantive). A majority (>50%) of its ultimate voting rights must be held by European entities or citizens, and no single non-EU entity may hold a "blocking minority" stake or exercise decisive influence through other means (e.g., special board rights, technology licensing dependencies).
- **Justification & Threat Model:** Formal EU domicile is insufficient if a non-EU entity can steer a provider's decisions to align with non-EU interests, effectively bypassing the domicile rule. This criterion closes the "Irish subsidiary" loophole, ensuring that the provider's governance and strategic direction are genuinely European.

Criterion 1.3: Jurisdictional Supremacy

- **Objective:** To verify that the provider is structurally and legally insulated from the extraterritorial reach of non-EU laws.
- **Core Requirement:** The provider must be legally structured to be exclusively subject to European law. It must demonstrate that its service delivery and core intellectual property are not dependent on non-European export controls or restrictive IP licenses that could be used as a geopolitical lever to disrupt service to European customers.
- **Justification & Threat Model:** A provider can be legally European but remain a technological vassal. The threat is a non-EU government using export controls or IP licensing as a weapon to coerce a provider or its customers. This criterion ensures the provider's legal structure and intellectual property do not create an additional vector for foreign coercion.

II. TECHNICAL SOVEREIGNTY (Core Guarantee)

Core Question: *Does the technology empower or encage the customer?*

This dimension is the antidote to the "sovereign prison". It ensures that Europe's digital infrastructure is built on a foundation of openness and freedom, guaranteeing long-term autonomy.

Criterion 2.1: Interoperability, Portability, and Use of Open Source Software

- **Objective:** To ensure customer freedom and prevent vendor lock-in.
- **Core Requirement:** The service must be built on open standards and predominantly use **Open Source Software** (using OSI-approved licenses) for its core components. The provider must guarantee data and workload portability, contractually prohibiting punitive data egress fees or other lock-in tactics.
- **Justification & Threat Model:** The threat is a secure but proprietary system where customers are trapped. Vendor lock-in allows a provider to unilaterally raise prices or degrade service. Open Source is the ultimate guarantee of freedom, providing the legal right to inspect, modify, and even "fork" the code, ensuring Europe can "stay by choice, not by lock-in."

Criterion 2.2: Architectural Transparency

- **Objective:** To ensure the service is not an unauditable "black box" and can be independently assessed.
- **Core Requirement:** The complete source code for all core technology components must be available for inspection, either publicly or via a trusted European third-party escrow. All deployed software must be verifiably reproducible from this audited source code.
- **Justification & Threat Model:** The threat is undisclosed vulnerabilities or backdoors hidden within opaque, closed-source systems. In a high-assurance environment, trust must be replaced by verifiable proof.

Criterion 2.3: Operational Reversibility

- **Objective:** To ensure service continuity beyond the provider's own viability, turning a service into a transferable industrial capability.
- **Core Requirement:** The service must be comprehensively documented and automated (e.g., Infrastructure-as-Code) to a degree that allows a competent third party to redeploy, configure, and operate it. A contractually binding exit plan is mandatory.

- **Justification & Threat Model:** The threat is provider failure (e.g., bankruptcy, acquisition by a non-EU entity). True sovereignty means a customer's critical operations are not existentially dependent on a single provider's survival.

III. OPERATIONAL SOVEREIGNTY (Core Guarantee)

Core Question: *Who has control over the operational environment?*

This dimension ensures that the entire operational chain—from the physical hardware to the system administrator - is under European control.

Criterion 3.1: EU Infrastructure and Control Plane

- **Objective:** To verify that the entire technical environment is physically located and operated from within the European Territory.
- **Core Requirement:** All physical infrastructure (datacenters, networks) and, critically, the **operational control plane** used to manage and orchestrate the service, must be located and operated exclusively from within the European Territory.
- **Justification & Threat Model:** This closes a major loophole where data can reside in the EU but be managed from outside. A non-EU control plane represents a direct, privileged access vector that bypasses all other jurisdictional and data residency protections.

Criterion 3.2: Exclusive European Personnel

- **Objective:** To ensure no non-European resident can exercise privileged access over the service's infrastructure or data.
- **Core Requirement:** 100% of personnel with privileged access to the service infrastructure and customer data must be residents of the European Territory, employed by a European Entity, and perform all their duties exclusively from within the European Territory.
- **Justification & Threat Model:** This creates a "human firewall". The threat is a privileged user located outside the EU who can be legally compelled by their local authorities to access data or alter the system, directly violating EU law.

IV. DATA SOVEREIGNTY (Core Guarantee)

Core Question: *Is the data verifiably protected, both legally and technically?*

This dimension provides tangible proof of data protection, moving beyond mere contractual promises to technical and legal enforcement.

Criterion 4.1: Exclusive EU Data Residency

- **Objective:** To verify that all customer data, in all its forms, remains physically and legally within the European Territory at all times.
- **Core Requirement:** All customer data—including primary data, backups, logs, and all associated **metadata**—must be stored and processed exclusively within the physical territory of the European Territory. No data, in any form, may be transferred or made accessible outside this territory.
- **Justification & Threat Model:** This bright-line rule closes loopholes related to metadata or backups being processed outside the EU, which could expose sensitive information even if the primary data is protected.

Criterion 4.2: Technical Data Access Protection

- **Objective:** To provide strong, state-of-the-art cryptographic protections that prevent unauthorized data access.
- **Core Requirement:** The service must offer, and contractually commit to, using verifiable technical measures, such as end-to-end **confidential computing or customer- exclusive cryptographic key management**, to prevent any party (including the provider) from accessing unencrypted customer data.
- **Justification & Threat Model:** This addresses the threat of a malicious insider or a provider being legally compelled to access customer data. Technical enforcement, where the provider is cryptographically unable to access data, provides a higher level of assurance than legal promises alone.

V. ECONOMIC SOVEREIGNTY (Key Differentiator)

Core Question: *Is the provider a net contributor to, or an extractor of value from, the European economy?*
This dimension serves as a powerful differentiator to select providers who are not just suppliers, but true strategic partners in building Europe's digital industrial base.

Criterion 5.1: European Value Creation

- **Objective:** To verify that intellectual property, strategic innovation, and high-value skills are developed and maintained in Europe.
- **Core Requirement:** The provider must demonstrate that the majority (>50%) of its global expenditure and personnel in **Research & Development** for the service's core technology are located within the European Territory.
- **Justification & Threat Model:** The threat is Europe becoming a "digital colony" - a mere consumer market where value is extracted rather than created. This ensures that the IP and high-value skills that drive the digital economy are developed and retained within Europe.

Criterion 5.2: Fair and Transparent Business Model

- **Objective:** To verify that the provider promotes healthy competition and does not use proprietary lock-in as a tool of strategic dependency.
- **Core Requirement:** The provider's business model must be transparent and explicitly prohibit punitive **data egress fees**, tied-selling, and other commercial lock-in tactics.
- **Justification & Threat Model:** Punitive egress fees are not just commercial issues; they are strategic barriers that prevent the emergence of a competitive and resilient European market.

Criterion 5.3: Commitment to the European Ecosystem

- **Objective:** To verify that the provider actively strengthens the resilience and competitiveness of the European digital ecosystem.
- **Core Requirement:** The provider must provide verifiable evidence of a substantial and continuous commitment to the European ecosystem, including active partnerships with European SMEs and significant, regular contributions to relevant **Open Source** projects.
- **Justification & Threat Model:** The threat is a single provider becoming a dominant, self-contained "walled garden". True resilience comes from a rich, collaborative ecosystem. This criterion ensures a provider acts as a responsible citizen, fostering collective strength.