19/11/2025

Clever Cloud Position Paper On the European Commission's Cloud Sovereignty Framework (CSF)

By Leo Le Levé Dandé

Company

Founded in 2010 in Nantes, France, Clever Cloud has established itself as a prominent player in the European cloud computing landscape, specializing in innovative Platform as a Service (PaaS) solutions. Our core mission is to empower developers by providing a reliable, scalable, and secure infrastructure that enables seamless application development, deployment, and management.

Clever Cloud is firmly committed to the principles of digital sovereignty, European values while advocating for a resilient and strategically autonomous digital ecosystem. We believe that Europe must prioritize its digital ecosystem to ensure that businesses and public authorities can operate independently without reliance on inadequate non-European solutions. Our expertise, underscored by a workforce composed of over 60% developers and engineers, positions us as a company of experts dedicated to both technical excellence and strong ethical European values.

As an active participant in the European legislative framework, Clever Cloud engages with critical initiatives aimed at enhancing Europe's digital sovereignty. We contribute to the development of key frameworks such as the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the EU Cybersecurity Act and of course The EU Cloud and AI Development act among others… Our involvement in organizations like Eurosmart, the Open Internet Project, and CISPE reflects our commitment to advocating for robust European certification schemes and ensuring that the cloud infrastructure respects and protects user rights. Through partnerships with leading European technology firms while preserving market freedom, we are building a cohesive digital ecosystem that fosters innovation, real free competition while preserving individual freedoms. Our dedication to creating and contributing to open-source projects further demonstrates our belief in collaboration as a means to strengthen Europe's digital sovereignty.

At Clever Cloud, we recognize that true digital sovereignty is essential for economic resilience and technological independence. By championing strategic policies and fostering a community of like-minded stakeholders, we are committed to shaping a future where Europe's digital landscape remains robust, secure, and innovative. Clever Cloud is delighted to contribute to the ongoing reflection on the European Cloud Sovereignty Framework, recognising its vital role in reinforcing Europe's digital strategic autonomy and in creating a coherent environment that supports innovation, competitiveness, and ethical technological practices. We also welcome the Commission's commitment to providing EU-level clarity and shared definitions around key concepts

1. A Welcome Initiative That Shall Become Regulatory

Clever Cloud welcomes the publication of the Cloud Sovereignty Framework (CSF) by the European Commission.

We see this as a first and meaningful step toward a genuine European Digital Agenda.

Until recently, **digital sovereignty was often regarded as a philosophical or political notion** — abstract, aspirational, and difficult to translate into practice.

With the publication of the **Sovereignty Framework**, it has now become a **technical and operational concept**, grounded in measurable criteria, structured governance, and transparent evaluation.

The next step must therefore be regulatory: transforming this conceptual and technical foundation into **binding European law** to ensure consistency, accountability, and legitimacy across Member States.

While the binding effect of the framework remains limited at this stage, it can — and should — serve as the foundation for a future regulatory and legally binding framework that will establish clear, enforceable sovereignty criteria across the Union.

It represents a positive and necessary milestone in operationalizing Europe's digital sovereignty within public procurement.

Indeed, although the CSF currently applies in the context of a call for tender rather than a formal consultation, this practical implementation demonstrates its potential for broader regulatory adoption.

If the European Union truly aims to secure its digital strategic autonomy, the framework must now evolve into a regulatory instrument, fully embedded within the EU Cybersecurity Certification Framework (EUCS) and aligned with the forthcoming revision of the Cybersecurity Act (CSA).

The debate around the EUCS dates back to the first draft published by ENISA in December 2020. After several years of technical discussions and political hesitation, the Council of the European Union, in September 2024, urged to move forward and break the deadlock, calling for the swift adoption of a balanced and operational certification scheme for cloud services in Europe. We consider that the regulatory path — through the formal integration of the Cloud Sovereignty Framework (CSF) into the EUCS — provides precisely the means to overcome the current stalemate and ensure decisive progress toward a coherent and enforceable European certification framework.

As a matter of fact, Clever Cloud supports both key mechanisms of the CSF, recognising the need for a multi-level framework that will also need to be reflected in the upcoming CSA revision and EU public procurement reform:

The Sovereignty Effective Assurance Levels (SEAL) as binding eligibility thresholds.

We strongly value the qualitative dimension of this mechanism — it acknowledges that while not every criterion can be expressed quantitatively, certain conditions are sine qua non.

This is particularly true regarding compliance with the GDPR, and the need to ensure that services are not subject to extraterritorial laws — a domain where a binary, yes-or-no approach is both justified and necessary.

The Sovereignty Score as a complementary evaluation and ranking tool.

We appreciate its contribution to a more quantitative and balanced assessment, enabling fair comparison and rewarding continuous improvement among cloud providers.

Beyond its conceptual soundness, one of the most commendable aspects of the CSF is its clarity and accessibility.

It provides a structured, multi-level model that translates complex notions of sovereignty into tangible and measurable objectives.

The combination of SEAL thresholds and a weighted scoring system makes it both feasible and user-friendly, offering a clear roadmap for compliance.

Importantly, the framework's design ensures accessibility for all cloud providers, not just the largest global actors.

By being transparent, progressive, and adaptable, it enables European and SME cloud providers to understand, assess, and gradually strengthen their sovereignty posture.

This accessibility represents a significant step toward the democratization of sovereignty compliance — lowering barriers to entry, fostering fair competition, and allowing public buyers to evaluate offers on objective, transparent criteria.

In that sense, the CSF contributes directly to building a more open, competitive, and inclusive European cloud ecosystem, where sovereignty becomes not an exclusive status reserved for a few, but a shared and attainable standard for all responsible providers.

2. The Urgent Need to Conclude the Sovereignty Debate

The debate on sovereignty within the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) has been ongoing since **December 2020.**

Nearly five years later, this regulatory discussion remains unresolved, delaying the establishment of a coherent European approach to digital sovereignty.

This situation can no longer continue.

In September 2024, the Council of the European Union explicitly urged the Commission and ENISA to accelerate progress and to provide a clear, harmonized framework for incorporating sovereignty criteria into the EUCS.

This political signal underscores a growing consensus: **As a matter of fact Clever Cloud consider that the regulatory path — through the formal integration of the Cloud Sovereignty Framework (CSF) into the EUCS — provides precisely the means to overcome the current stalemate and ensure decisive progress toward a coherent and enforceable European certification framework.**

Rather than reopening technical arguments, the focus should now be on transposing the principles of the Cloud Sovereignty Framework (CSF) into **the regulatory domain.**

The CSF provides an operational and policy-ready model that can give political meaning to the EUCS, transforming it from a purely technical scheme into an instrument that reflects **Europe's broader sovereignty objectives.**

Once the regulatory integration of sovereignty is achieved within the EUCS, the question of metrics can be addressed in a multi-level governance framework — under ENISA's coordination, with the involvement of Conformity Assessment Bodies, Notified Bodies, independent authorities, and industry experts.

This is how Europe can ensure both technical credibility and political legitimacy, turning the EUCS from a stalled discussion into a functioning pillar of European sovereignty.

3. Legal Dimension – Addressing the US Extraterritoriality But not only

Sovereignty cannot be achieved without explicitly addressing extraterritorial legal exposure. The SOV-2 Legal & Jurisdictional Sovereignty pillar must acknowledge and quantify the risks stemming from foreign laws with global reach, including but not limited to:

- **U.S. CLOUD Act and FISA Section 702,**
- **China's Cybersecurity Law and PIPL,**
- **India's Digital Personal Data Protection Act,**
- **Brazil's LGPD,**
- **Japan's APPI,**
- **The Russian Federal Law No. 152-FZ (Personal Data Law)**
- **And other similar third-country frameworks with extraterritorial claims.**

Europe's challenge is no longer limited to U.S. jurisdiction — it is **systemic and global**. The CSF, if anchored in EUCS, can become the instrument to **identify and exclude dependencies** that expose European data and infrastructure to such foreign legal risks.

It is particularly critical that the FISA 702 framework be more explicitly addressed within the EUCS context. Unlike the U.S. CLOUD Act — where limited judicial recourse may exist — FISA 702 provides no possibility of appeal or notification. Technology companies subject to U.S. jurisdiction are legally compelled to grant access to data, even when that data belongs to non-U.S. persons and is hosted outside U.S. territory. Moreover, they are prohibited from informing clients that such access has occurred.

Companies under U.S. jurisdiction are **legally compelled to provide access** to data, including that of **non-U.S. persons stored outside the United States**, and are simultaneously **forbidden from disclosing** that such access has occurred.
In practice, this creates a situation in which the **National Security Agency (NSA)** occupies a position of **supremacy within the U.S. legal hierarchy**, effectively overriding contractual, national, or even international data protection commitments.
Such a configuration stands in **direct opposition to the European Union's foundational principle of the Rule of Law**, where all public power must remain subject to legal accountability and judicial oversight.

Most importantly, **FISA 702 is fundamentally incompatible with Article 48 of the GDPR**, which stipulates that:

"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable […] if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State."

FISA 702 **bypasses this legal safeguard entirely**. It authorizes unilateral access by U.S. intelligence agencies **without any mutual legal assistance mechanism** or **international agreement** with the European Union.

This absence of reciprocity and external oversight renders compliance with both **FISA 702** and the **GDPR mutually exclusive**. Therefore, under the principle of legal sovereignty and the hierarchy of norms established by EU law, **any entity subject to FISA 702 cannot simultaneously guarantee GDPR-compliant data protection**. Recognizing this contradiction within the EUCS is essential to preserve the **integrity, legality, and credibility** of Europe's sovereign cloud certification framework.

4. Metrics Must Be Defined Within the Regulatory Framework

Defining sovereignty metrics — the evidence, scoring weights, and thresholds — cannot rely solely on procurement discretion.

It must occur within a regulated, auditable, and harmonized framework, involving:

- **Conformity Assessment Bodies (CABs),**
- **Notified Bodies,**
- **independent EU-supervised authorities, and**
- **expert committees operating under the EUCS and CSA frameworks.**

Beyond establishing a governance framework and evaluating criterias, this process must also be supported by a robust and transparent methodology. Such a methodology should:

- Combine quantitative and qualitative criteria, ensuring that assessments capture both measurable compliance aspects and contextual or strategic dimensions of sovereignty;
- Adopt an approach similar to SEAL + Scoring, allowing for harmonized, evidence-based evaluation and progressive improvement of sovereignty maturity levels;
- Clearly define which types of services and data require a sovereign cloud, and which do not, in order to avoid overreach and ensure proportionality between regulatory objectives and operational needs.
- Ensure that sovereignty assessments complement, and do not substitute, cybersecurity and compliance requirements, particularly those established by European legislative acts such as the Cyber Resilience Act (CRA).
- In particular, Article 3 of the CRA, which addresses remote data processing, must be considered a key interoperability point: sovereignty evaluation should integrate or align with these robustness and security expectations to ensure a coherent and comprehensive regulatory approach across all dimensions — cybersecurity, compliance, and sovereignty.

Hence, only such governance and methodological rigor can guarantee:

- **Consistent interpretation of sovereignty criteria,**
- **mutual recognition of assessments across Member States, and**
- **Legitimacy and reliability of certification at European level.**

This approach would ensure that the CSF and EUCS form a coherent architecture:

- In other words, **The CSA (Cybersecurity Act)** provides the legal foundation — the European framework for cybersecurity certification, under which schemes like EUCS are established and supervised by ENISA and the Commission while
- **The EUCS (European Cloud Services Scheme)** is the operational layer — the certification scheme that translates the high-level regulatory goals of the CSA into concrete, measurable requirements for cloud service providers.
- The CSF has to be used as a fitting step to define the "what" (sovereignty principles, dimensions, criteria). Meanwhile… The EUCS, under the CSA, defines the "how" (certification, metrics, conformity, assessment).

5. From Procurement to Regulation – Anchoring CSF in the CSA Revision

The **revision of the Cybersecurity Act (CSA)** is the natural regulatory home for the CSF.
The CSA already mandates the creation of **EU-wide certification schemes** (EUCC, EU5G, EUCS).
Integrating the CSF's sovereignty layer within the revised CSA would:

- **End the ongoing sovereignty debate**,
- Give **legal certainty** to contracting authorities and cloud providers,
- And ensure that sovereignty requirements become **binding, measurable, and enforceable**.

This alignment would also bridge the **current gap between procurement practices and regulatory frameworks** — ensuring that future tenders are not isolated exercises, but **applications of EU law**.

The European Commission has already launched the **consultation on the revision of EU public procurement rules (2026)**, as announced in **President von der Leyen's 2024–2029 political guidelines**.
This upcoming reform aims to:

- **Enable preference for European products and technologies** in public procurement,
- **Secure the supply of vital services and infrastructures**,
- **Modernise and simplify procurement procedures**, and
- **Transform public procurement into a tool for strategic investment**, strengthening the Single Market.

This reform provides a **unique opportunity to anchor the CSF into EU law**.
While the **Cloud Sovereignty Framework** currently applies as a **procurement procedure** internal to the Commission, the **2026 revision should elevate these principles to a legal standard** across all public buyers in the Union.

In practical terms:

- **Sovereignty criteria (SEAL + Score)** should become **mandatory reference points** in EU public procurement for cloud and digital services;
- The **EUCS certification framework**, developed under the **Cybersecurity Act**, should be **explicitly referenced** as the **verification mechanism** for compliance with those sovereignty requirements;
- The **CSA revision and the Public Procurement revision must therefore advance in parallel**, establishing a **direct regulatory link** between **certification, conformity assessment, and procurement eligibility**.

6. The Environmental and Scoring Dimensions Must Be Preserved

Clever Cloud firmly opposes any proposal to remove the **scoring mechanism** or the **environmental sustainability objective (SOV-8)**.
Both are integral to sovereignty.

- The **scoring system** introduces a culture of **progressive improvement** and transparency.
- The **environmental dimension** is a matter of **strategic independence**: energy efficiency, supply resilience, and lifecycle management are all sovereignty issues.

Eliminating these dimensions would contradict the goals of the **Cloud and AI Development Act**, which explicitly links **sustainability and autonomy** as drivers of European competitiveness.

Beyond compliance, this approach embodies genuine eco-responsibility.

By promoting energy efficiency, hardware lifecycle optimization, and reduced resource waste, the framework encourages providers to minimize environmental impact while reinforcing Europe's strategic autonomy in energy and digital infrastructure. Sustainability thus becomes not only an ethical imperative but a sovereignty enabler, ensuring that European cloud services remain both resilient and responsible in the face of global resource and energy constraints.

Clever Cloud is fully committed to this vision. We are ready to demonstrate how our Platform-as-a-Service (PaaS) model inherently supports these environmental and sovereignty goals — through optimized resource allocation, automation-driven efficiency, and reduced idle capacity.

This architecture naturally limits overprovisioning and energy waste, ensuring that computational resources are used only when needed. By design, our PaaS offering aligns with the principles of the upcoming Cloud and AI Development Act, combining environmental sustainability, operational sovereignty, and European competitiveness within a single, coherent framework.

7. Clever Cloud's Recommendations

- **Formally integrate** the **Cloud Sovereignty Framework (CSF)** into the **EUCS certification scheme** under the **revised Cybersecurity Act (CSA)**. This integration must **conclude the sovereignty debate** by establishing **clear, auditable legal, operational, and supply-chain sovereignty criteria**, applicable across all Member States.
- **Develop sovereignty metrics and methodologies** within the **EU's regulatory process**, under the coordination of **ENISA**, and in collaboration with **Conformity Assessment Bodies (CABs)**, **Notified Bodies**, and **expert working groups**. A **structured, quantitative and qualitative methodology** should define how sovereignty is measured, scored, and continuously improved.
- **Adopt an inclusive governance model**. Establish a **formal consultation process or call for evidence** to ensure the participation of all stakeholders — cloud providers, SMEs, public authorities, civil society, and research actors — and to **end the current fragmentation of opinion leaders** on sovereignty.
  This initiative could be anchored in existing forums, such as the **Working Group on Cybersecurity and Data Protection** of the **European Digital SME Alliance**, ensuring that **SME perspectives** are properly represented in the legislative and technical design of sovereignty standards.
- **Use CSF–EUCS integration as the operational backbone** for **certifying sovereign cloud offers** across Europe. Preserve both the **scoring methodology** and the **SOV-8 environmental objective**, ensuring that sovereignty remains a **multidimensional concept** — legal, operational, and environmental — rather than a geopolitical label.
- **Ensure coherence between public procurement and certification**. Future **public tenders** should directly apply **binding sovereignty standards** defined through EUCS, creating a **level playing field** and **legal certainty** for all actors.
- **Prevent "sovereign washing."**. The **European Commission** must actively address **extraterritorial risks** posed by foreign surveillance laws such as the **U.S. CLOUD Act** and **FISA Section 702**. While the **CLOUD Act** introduces ambiguities in GDPR compliance, **FISA 702** fundamentally **contradicts Article 48 of the GDPR**, which stipulates that: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable […] if based on an international agreement." **FISA 702** authorizes unilateral data access by U.S. intelligence agencies to data belonging to **non-U.S. persons**, even when hosted **outside U.S. territory**, without **judicial reciprocity, transparency, or EU oversight** — a clear breach of **GDPR principles** and the **EU legal order**. A truly sovereign certification framework must therefore **explicitly exclude providers subject to such extraterritorial legislation**, anchoring **sovereignty as a legal condition for trust** within the **European Digital Single Market**.
- In a rapidly evolving technical and regulatory environment, ensuring **the ongoing maintenance of both the framework and the sovereignty criteria** requires a structure that integrates the expertise of cloud professionals and public authorities. In this regard, **the ISAC model** – designed as a public-private partnership – stands out as a particularly relevant approach.

8. Conclusion – From Framework to Regulation

During the Summit on European Digital Sovereignty in Berlin, **German Chancellor Friedrich Merz emphasized** that the event marks an essential milestone on the path toward a more sovereign, secure, and competitive digital Europe. On the French side, President Emmanuel Macron underscored that this sends a clear signal: **Europe has what it takes to lead the digital age**.

The **Cloud Sovereignty Framework** is a milestone — but as a matter of fact it must not remain a voluntary or procedural tool. Its real potential lies in becoming **the regulatory foundation** for European digital sovereignty.

The **revision of the Cybersecurity Act** is the decisive moment to do so.
By integrating the CSF into the EUCS certification scheme, the Commission can **end the political stalemate on sovereignty**, provide **clarity to the market**, and ensure that **European data and infrastructures are governed exclusively under EU law**.**Clever Cloud stands ready to contribute** to this process and stands ready to contribute actively, offering its technical expertise to help shape a robust and sovereign framework— bringing the perspective of an independent, transparent, and fully European cloud provider committed to a sustainable and sovereign digital Europe.

BLOG

À lire également

19/11/2025
Clever Cloud Position Paper On the European Commission's Cloud Sovereignty Framework (CSF)
Founded in 2010 in Nantes, France, Clever Cloud has established itself as a prominent player in the European cloud computing landscape, specializing in innovative Platform as a Service (PaaS) solutions. Our core mission is to empower developers by providing a reliable, scalable, and secure infrastructure that enables seamless application development, deployment, and management.
Company

10/11/2025
Manage your WordPress identities with Keycloak
Managing logins to your website can be a complex task. Fortunately, tools like Keycloak, an open-source Identity and Access Management (IAM) solution, can make it much easier to handle authentication and authorization for your application.
Engineering

06/11/2025
Clever Cloud launches its first certification: "Cloud Concepts 101"
Clever Cloud, a leading European provider of Platform as a Service (PaaS) solutions, announces the launch of its first official certification, Cloud Concepts 101, designed to help developers master the fundamentals of cloud computing and the Clever Cloud platform.
Company