

ESTIA initial position on the Cloud and AI Development Act

ESTIA's key asks

ESTIA welcomes CADA as a decisive step towards strengthening Europe's cloud and AI ecosystem and operationalising the EU's cloud sovereignty agenda.

ESTIA calls on the European Parliament and Council to preserve and strengthen the proposal's ambition by ensuring that the final Regulation:

1. maintains a clear, auditable, future-proof, harmonised and binding cloud sovereignty framework within CADA;
2. ensures that sovereignty over data is complemented by sovereignty over the service;
3. makes the highest Union assurance levels meaningful for sensitive public-sector data and workloads;
4. uses public procurement and "EU added value" criteria as a strategic lever for European competitiveness, with sufficient weight in tenders;
5. ensures that critical public-sector data and workloads are tendered to European sovereign cloud providers;
6. supports open-source solutions, open cloud stacks and EU-controlled software capabilities as key drivers towards full resilience.
7. Prioritises strategic data centre projects for new or expanding European-controlled capacity

CADA is a decisive opportunity. ESTIA stands ready to work constructively with the European Commission, European Parliament and Council to ensure that the final Regulation delivers on Europe's need for secure, resilient and competitive sovereign cloud solutions.

A decisive opportunity to strengthen Europe's cloud and AI sovereignty

Europe is reaching a critical moment for its digital sovereignty. Today, nearly 90% of EU data is transferred to third countries, while non-European providers dominate the European cloud market. This growing dependency creates significant risks for Europe's economic resilience, security, and technological autonomy.

ESTIA welcomes the Commission's proposal for a Cloud and AI Development Act (CADA). The proposal is timely, ambitious and necessary. It recognises that cloud and AI are foundational to Europe's economy and competitiveness, and that Europe's digital sovereignty requires both investment in European capabilities and a stronger demand base for European sovereign cloud services.

As European Industry leaders, we are observing a rising demand for EU-sovereign cloud services for specific data and critical usages. The need behind this relates to ensuring that services cannot be

disrupted by non-EU extraterritorial legislation or influence, notably in terms of undue access to data or the quality and availability of the service provided.

Europe already has the capability to deliver secure, resilient and competitive sovereign cloud solutions. European cloud providers are already providing trusted, highly performant and innovative services today, designed to meet European organisations' highest standards for data protection, resilience and sovereignty.

ESTIA therefore supports the direction of CADA and calls on the co-legislators to preserve and strengthen its ambition.

1. ESTIA welcomes CADA's integrated approach

ESTIA welcomes that CADA addresses the cloud and AI challenge through a coherent European industrial policy approach, combining investment in European capabilities with demand-side measures that allow European technologies to scale.

ESTIA supports the proposal's efforts to:

- establish a European cloud sovereignty framework based on Union assurance levels and common criteria;
- link sovereignty requirements to public procurement for critical public-sector activities;
- strengthen Europe's cloud and AI ecosystem through the Cloud and AI Leadership Initiatives;
- expand data centre capacity through acceleration zones, streamlined permitting and strategic project designation;
- promote open-source solutions, software reuse and open cloud stacks as a lever for technological sovereignty.

Taken together, these measures can help position Europe as a global hub for trusted, sovereign and scalable digital infrastructure.

2. The cloud sovereignty framework is a major step forward

ESTIA strongly welcomes the establishment of a Union cloud computing sovereignty framework in Title IV, Chapter I of CADA, including the recognition of cloud computing service providers under Article 17 and the Union assurance levels under Article 16 and Annex II.

There is a need for an EU-wide unified framework to measure cloud sovereignty, avoiding unnecessary overlap or diverging systems. Such a framework should be cloud-specific and based on CADA.

ESTIA therefore calls on the co-legislators to ensure that CADA reflects two complementary levels of sovereignty:

A. Data and operational sovereignty, based on:

- jurisdictional control under European law, including absence of non-EU control, protections against change of control and the prevalence of EU law;
- data localisation and processing within the EU and EFTA;
- operational independence, meaning that a non-EU subcontractor must not have the ability to cut off access to the service, or that the provider can continue providing the service using its own resources or alternative providers.

B. Service resilience, through a gradual approach, based on:

- EU control over intellectual property, including access to the source code or the ability to substitute with an open source or EU alternative;
- ability to deploy security patches and upgrades autonomously;
- execution of the software stack under the control of an EU-controlled provider.

CADA's Union assurance levels provide a useful basis for this approach. ESTIA supports a differentiated architecture of audited assurance levels and encourages the co-legislators to ensure that the highest levels are meaningful, enforceable, auditable and aligned with the objective of protecting sensitive public-sector data and workloads against extraterritorial laws, undue access to data and service disruption. The framework should prevent sovereignty washing by clearly distinguishing between baseline requirements applying to all providers and sovereignty requirements ensuring that demand for higher-assurance services supports genuinely sovereign, EU-controlled solutions.

The Article 18 mechanism for associated third countries should be implemented in a way that preserves the core sovereignty objective of CADA and remains conditional on equivalent safeguards, as to ensure that recognition as sovereign requires genuine European legal and operational control.

3. Public procurement must become a strategic lever

ESTIA welcomes that CADA recognises public procurement as a strategic lever for European competitiveness. Public procurement is one of the most important tools available to Europe to strengthen both the supply and demand side of the European cloud and AI ecosystem. The public sector should be anchor customers, stimulating the offer and demand needed for European technologies to scale.

ESTIA therefore strongly supports CADA's demand-side measures, in particular:

- Article 29, requiring Member States and Union entities to identify activities requiring sovereign cloud services through risk assessments conducted on the basis of Commission guidance;
- Article 30, linking public procurement of cloud computing services to the relevant Union assurance levels;
- Article 32, introducing Union added-value criteria in procurement of cloud computing services and AI systems, with sufficient weight to be a meaningful factor;

- Articles 34 to 40, providing for a European public sector cloud federation and Commission-led procurement activities.

These provisions are essential because developing competitive sovereign cloud services requires predictable demand. Introducing a European preference for cloud data and workloads would strengthen both the supply and demand side by nurturing a robust European industrial base, stimulating homegrown innovation and making public institutions the anchor customers for European solutions.

The final CADA should therefore establish a clear European preference framework for future cloud use in the public sector. In practice, ESTIA calls for:

1. 100% of critical public-sector data and workloads to be tendered to European sovereign cloud providers, subject to strictly limited, duly justified and time-limited exceptions;
2. a significant part of the remaining public-sector data and workloads to be tendered to European cloud providers, with targets increasing over time;
3. public funding towards private companies involving cloud technologies to include a preference for European cloud operators.

ESTIA supports the logic of Article 30 and considers that exceptions should remain strictly limited, duly justified and transparent.

4. CADA should support full-stack resilience

ESTIA welcomes that CADA is embedded in the broader Tech Sovereignty Package. Full-stack technological independence remains the strategic objective. While some cloud functionalities and managed services remain of foreign origin, European companies and the open-source community have already built strong software capabilities.

ESTIA supports CADA's focus on open cloud stacks and open-source solutions, including Articles 41 to 43 on promoting open-source solutions, sharing and reuse of software, and the EU Open Source Solutions Catalogue. The Open Source Strategy can fill common gaps for all cloud service providers and reduce dependencies on a single vendor.

ESTIA also welcomes the proposal's data centre capacity measures in Title III. Acceleration zones, strategic project designation and capacity monitoring can help address Europe's infrastructure gap and support the capacity needed for sovereign cloud and AI development, and should prioritise projects for new or expanding European-controlled capacity.



About ESTIA

The European Sovereign Tech Industry Alliance (ESTIA) is a coalition of Europe's leading cloud, digital services, and technology companies driving the creation of a trustworthy, independent European digital ecosystem.