CloudFerro

CloudFerro position on the proposed Cloud and AI Development Act



European control over technology as a condition for an effective CADA

CloudFerro supports the objectives of the proposed Cloud and AI Development Act, in particular the expansion of European computing capacity, the development of cloud and AI infrastructure, and the strengthening of the European Union's technological resilience. The proposal can become an important instrument of European industrial policy, provided that its provisions bring about a meaningful change in market structure rather than merely increasing the number of data centres located in the EU and introducing new compliance labels.

CADA will be effective only if it distinguishes between infrastructure located in Europe and technology effectively controlled in Europe. The location of infrastructure, data or personnel within the Union does not in itself provide the capacity to develop, maintain and deliver key services independently. This capacity also depends on ownership and operational control, applicable jurisdiction, intellectual property, access to source code, control over updates and the absence of critical dependencies on third-country entities.

Europe needs providers capable of delivering and developing their services without requiring the consent of, or relying on technology or decisions controlled by, entities subject to third-country jurisdictions. CADA should therefore be based on four principles: European control rather than European location alone; public procurement as an industrial policy instrument; infrastructure and investment support linked to European autonomy; and measurement of actual changes in market structure.

Strengthening European control should not be understood as a limitation of competition. On the contrary, it should create conditions for a more competitive, diversified and resilient European cloud and AI market.

1. European control, not merely European location

1.1. Distinguishing service assurance from the status of a European provider

CADA should clearly distinguish between a service meeting a given Union Assurance Level and a European-controlled provider. An assurance level should describe the characteristics of a specific service, including its security, resilience, location and operational control model. The status of a European-controlled provider should determine whether an entity is eligible for procurement preferences, public funding and strategic project status.

Not every secure service has to be provided by a European supplier. At the same time, not every provider offering a service that meets the applicable security requirements should benefit from European industrial policy instruments. Such instruments should support entities that create and maintain genuine technological, operational and decision-making capabilities in Europe.

1.2. Effective control test

Recognition as a European-controlled provider should be subject to a uniform effective control test. The test should apply whenever an entity seeks access to procurement preferences, public funding or strategic project status.

The assessment should cover at least:

- ownership and corporate control;
- voting and veto rights;
- the location of the actual decision-making centre;
- the jurisdiction applicable to the provider and its group entities;
- operational control over service delivery;
- the management of privileged access;
- intellectual property and control over source code and updates;
- the ability to maintain and develop the service independently;
- critical technological, financial and contractual dependencies.

An entity should not qualify as a European-controlled provider where the independent delivery or development of its service depends on licences, updates, source code, support or decisions controlled by a third-country entity. This should also apply to dependencies arising from licensing agreements, joint ventures, technical support arrangements or group structures.

Such a test is necessary to prevent sovereignty washing, whereby a provider formally meets certain location or corporate requirements while remaining technologically or operationally dependent on an entity established outside the Union.

1.3. AI and the full technology stack

Practical sovereignty requirements should not be limited to core cloud infrastructure services. They should also apply to AI-as-a-Service, AI platforms, inference services, model management and the data layer. The CADA framework should not provide significantly more developed

requirements for cloud services than for AI services if both are to be covered by the same instrument.

Providers should be required to disclose critical technological dependencies across the entire technology stack. The disclosure obligation should cover, in particular, orchestration and management layers, telemetry and update systems, identity management, control over cryptographic keys and other components controlled by third parties.

Location and control requirements should apply not only to customer data, but also to metadata, operational logs, telemetry and diagnostic information. The transfer of such information to infrastructure or entities controlled outside the EU can create dependencies and risks comparable to those concerning primary customer data.

1.4. Level 1 as a baseline compliance level

Union Assurance Level 1 should not be equated with sovereignty or marketed as a sovereign cloud certification. It should be designated as a European baseline compliance level. This distinction is necessary to prevent self-assessment from being used to support marketing claims implying a degree of control or autonomy that the provider does not in fact ensure.

Provider self-assessments should be subject to random checks and effective, proportionate penalties for false or misleading declarations. For the largest providers and entities controlled from third countries, Level 1 should require independent verification. Their scale, available resources and potential risk exposure justify a higher standard than the one applied to European small and medium-sized enterprises.

1.5. Audit and enforcement

The credibility of the assurance framework depends on the quality, independence and consistency of audits. Organisations conducting Level 3 and Level 4 audits should be established in the European Union, be subject to European control and have their key personnel performing the relevant functions within the EU.

Uniform accreditation requirements and a transparent European register of auditing organisations should be established at Union level. This would reduce regulatory arbitrage between Member States and the risk of certifications being issued according to different standards of quality and reliability.

The framework should allow unannounced audits and technical testing of declared separation, continuity and control mechanisms. Assessments should not be based solely on documentation submitted by the provider.

Providers should also be required to report data access orders, attempts to compel the disruption or restriction of a service, and other requests from third-country authorities that may affect the security, availability or control of the service. This obligation should apply to the provider itself and to all group entities involved in delivering the service.

2. Public procurement as an industrial policy instrument

Public procurement should be used to create predictable demand for solutions developed and controlled in Europe. Without appropriate demand-side measures, CADA may increase the number of available certifications and computing capacity without changing the market share of European providers.

The Union added value criterion should apply to all material procurement procedures concerning cloud and AI services, rather than only to procedures classified as innovative procurement. Its application should depend on the significance and subject matter of the contract, not on its formal classification.

The provision under which the Union added value criterion cannot determine the outcome of a procurement procedure should be removed. In strategic procurement, the criterion should account for at least 20–30% of the total award score. The assessment should take into account European control over the provider, intellectual property, the share of research and development conducted in Europe, the location of relevant capabilities and the provider's contribution to the European value chain.

A European preference or European first principle should apply to strategic public-sector use cases. Where a functionally comparable offer from a European-controlled provider is available, its selection should be the default outcome. Any departure from this principle should require a written justification made publicly available.

CADA should also establish a binding target under which at least 50% of public expenditure on cloud services is directed to European-controlled providers by 2034. Progress towards this target should be monitored at Union and Member State level and reflected in national procurement strategies.

Large contracts should, as a general rule, be divided into lots and allow multi-vendor architectures. A contracting authority should be permitted to depart from these principles only where it demonstrates that dividing the contract or applying a multi-vendor architecture would be technically or economically unjustified.

This approach would facilitate the participation of European providers in large procurement procedures, reduce dependence on individual suppliers and improve the ability to transfer workloads, substitute services and maintain operational continuity.

3. European infrastructure and investment autonomy

Increasing data-centre capacity in the European Union is necessary, but it should not be equated with greater European technological autonomy. Infrastructure located in the EU may remain controlled by third-country entities, rely on technologies developed outside Europe and reinforce the market position of non-EU providers.

Strategic data-centre project status should require a measurable contribution to European technological sovereignty. The provision of capital or the addition of computing capacity within the EU should not in itself be sufficient to obtain this status.

Public support should be directed towards increasing European ownership, control and technological capabilities rather than solely increasing capacity located within the Union.

Preferential financing, access to land, accelerated permitting procedures and support in securing access to energy should be linked either to European control over the infrastructure or to a long-term commitment to allocate a material share of computing capacity to European providers and strategic users.

The assessment of projects should take into account the European share of value added, in particular:

- research and development conducted in Europe;
- European personnel and capabilities;
- the use of European software and hardware;
- energy sourced in Europe;
- the project's tax contribution;
- the participation of local and European subcontractors.

A beneficiary of support for a strategic project should demonstrate how the project reduces Europe's technological dependencies. European funds should not support projects that merely relocate third-country-controlled infrastructure geographically or lead to a further increase in the market share of non-EU providers.

4. Extending the framework to critical private sectors

The CADA framework should not be limited to public administrations. A significant share of critical data, infrastructure and services is processed or operated by private entities. Leaving the application of assurance levels entirely to their voluntary decisions could result in different protection standards for comparable systems and data.

Mandatory risk assessments should apply to essential entities within the meaning of the NIS2 Directive, at least in healthcare, energy, finance, telecommunications, space and defence.

Minimum Union Assurance Levels should be established for defined categories of critical use cases. The required level should depend on the type of data, the function of the system, the consequences of service disruption and the degree of technological dependency, irrespective of whether the system is operated by a public or private entity.

5. Measuring actual market change

The effectiveness of CADA should not be measured by the number of certificates issued. Certification is an instrument for implementing policy, not an objective in itself. An increase in the number of services covered by assurance levels does not necessarily strengthen European technological capabilities or reduce market concentration.

The European Commission and the Member States should monitor, in particular:

- the revenue share of European providers in the European cloud and AI markets;
- the share of computing capacity under European ownership and effective control;
- the value of public contracts awarded to European-controlled providers;
- changes in the level of concentration in the European cloud and AI markets.

The Commission should also monitor the economic beneficiaries of CADA instruments. This assessment should cover public funding, preferential investment conditions, accelerated procedures, energy-related support, public procurement and strategic project status.

Without such monitoring, all regulatory processes established under CADA could be formally implemented while the market share of incumbent providers and Europe's technological dependencies continue to increase.

Conclusion

CADA can become a central instrument for developing the European cloud and AI ecosystem. To achieve this objective, the Regulation must go beyond the location of infrastructure and formal compliance labels. It should reward effective European control, use public procurement to shape the market, direct investment support towards projects that reduce technological dependencies and create conditions for cooperation between European providers.

CADA should not be assessed by the number of certified services, data centres built or compliance processes completed. Its success should be measured by whether it increases the share of European-controlled providers, strengthens Europe's capacity to independently develop and operate critical digital infrastructure, and reduces structural dependencies in strategically important sectors.

Europe needs more than additional data-centre capacity. Europe needs providers with the capabilities, technology and operational capacity to develop, maintain and deliver key services independently. Only then will CADA deliver its intended objective: a competitive, resilient and strategically autonomous European cloud and AI ecosystem capable of supporting Europe's digital economy, public sector and critical infrastructures.

tel. +48 22 354 65 73
office@cloudferro.com
www.cloudferro.com

HQ: ul. Fabryczna 5, 00-446 Warsaw, Poland
Registered office: ul. Nowogrodzka 31, 00-511 Warsaw, Poland
KRS: 0001049205 | **NIP:** 7010468205 | **Share capital:** 360,400.00 PLN (fully paid)