

CADA: A new proposal for digital sovereignty rules in the EU?

By Vincent WELLENS, Avocat à la Cour & Ottavio COVOLO, Avocat à la Cour, NautaDutilh Avocats Luxembourg Sàrl

On 3 June 2026, the EU Commission published a proposal for a regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem: the Cloud and AI Development Act, or "CADA". The proposal aims at providing legal instruments for the EU and the Member States to commit to actions to improve the competitiveness of the EU ecosystem in relation to AI, cloud systems, and data centres, whilst also furthering the digital sovereignty of the EU. How does this fit in the current landscape of EU regulations on the same topics and what does CADA actually bring to the table?

CADA, part of the wider EU Tech Sovereignty Package, was published together with three other initiatives: the "Chips Act 2.0" (which mobilizes funding in the area of semiconductors), the "EU Open Source Strategy" (not a legislative text but rather policy objectives to increase adoption and support of open-source software), and a "Strategic roadmap for digitalisation and AI in energy" (also a non-legislative text setting objectives to leverage technology for better efficiency of the energy grid).

Given the current geopolitical context, this package is yet another step in addressing the EU's structural dependencies on technology and services stemming from other countries, motivated by concerns of sovereignty and market competitiveness. As a competitiveness tool for EU players, it does not aim at regulating products and services with the indirect effect of excluding or hampering non-EU players, as some commentators saw with the GDPR. Rather, it directs the EU Member States to take concrete steps towards key technological objectives (so-called "grand challenges") through 3 main pillars.

Pillar 1: R&D and Data Centres

The CADA provides for the adoption of "Cloud and AI Leadership Initiatives" by the Commission and Member States, which consist of programmes in that area supported by EU funding, including Horizon Europe and the Digital Europe Programme. The CADA sets out in detail the different operational objectives that such initiatives may serve, whilst emphasising that they should be consistent and coherent with other existing initiatives at the EU level. The proposal refers for instance to the objective of "tripling the EU's data centre capacity within the next five to seven years" whilst also increasing "the adoption



of cloud computing services across the public sector". The Commission is also empowered to designate "frontier priority projects" to receive further support in tackling the "grand challenge" of developing "the next generation of multimodal frontier AI models and systems and pioneering novel capabilities".

Member States are also tasked with setting up "Experience and Acceleration Centres for AI" in line with structures of innovation hubs introduced with the Digital Europe Programme. Member States must in addition adopt specific cloud and AI strategies consistent with CADA, meaning that the Luxembourg "Accelerating digital sovereignty 2030" strategic initiative may need to be tweaked as a result.

CADA also aims at facilitating data centre developments. Member states must designate at least one "data centre acceleration zone", where data centre projects will benefit from streamlined permitting processes (through notably a single contact point put in place by the Member State for all communications), aggregated baseline permits, and a maximum 12-month permit-granting timeline. The Commission may also designate certain data centre projects as "strategic projects" in certain circumstances, enabling them to benefit from additional public support measures and preferential access to EU funding instruments.

These provisions present both opportunities and potential constraints for hyperscalers and other cloud and AI service providers. The acceleration zones and streamlined permitting could significantly reduce the time and cost of deploying new facilities, but the emphasis on sustainability requirements, the preference for brownfield over greenfield sites, and the conditions for grid connection will shape investment decisions. The streamlined administrative process may add further pressure on the challenges Luxembourg is currently facing in relation to building permits and the administrative procedures related thereto. This being said, the future introduction of the "once only" principle not required by CADA may bring a competitive advantage when compared to other Member States.

Pillar 2: Autonomy, or the Cloud Sovereignty Framework

The key element of CADA, and reportedly likely source of discussion in the upcoming trilogue discussions, is the introduction of a cloud EU assurance scheme, similar to ISO and the CSA Star ones, but focused on ensuring digital sovereignty.

By way of background, this comes after initiatives such as in France or Germany to consider sovereignty issues when procuring services (the "Cloud de Confiance" and "Souverain Cloud" strategies respectively), and the Commission's own Cloud Sovereignty Framework also aimed at including a sovereignty score in public procurements.

This is not to be confused with the other existing EU cybersecurity certification scheme ("EUCC") focused solely on cybersecurity. Although, as discussed previously in our February article, the underlying rationale of cybersecurity is also reflective of geopolitical tensions in ensuring digital resilience, meaning controlling supply chains whilst mitigating the risk of foreign interference.

The cloud EU assurance scheme, however, includes a mechanism of trusted third States, or "Associated Third Countries", similar to the GDPR's adequacy decisions, which are even one of the pre-requisites, in addition to the absence of any "illegitimate" measures to compel the cloud service provider to stop providing services, including for sanctions-related obligations.

CADA furthermore includes consequences in cases of breaches of the rules regarding the framework, e.g., cases of misrepresentation towards customers. Entities in breach may face penalties from Member States, which are free to decide on administrative and/or criminal fines depending on their national law, with Luxembourg expected to provide only administrative fines given the approach taken in other laws on the subject matter. Customers of entities are also provided the explicit right to seek damages or loss suffered as a result of said infringement "in accordance with Union and national law". Careful consideration should therefore be given to the exact scope of the assurances (which could amount to contractual warranties), since they could override any waiver or exclusion of liability provided in terms and conditions of cloud service providers.

Pillar 3: Public procurement

The cloud security framework will become a mandatory part of public procurements, with an explicit obligation for member States (alone or jointly) to identify through risk assessments whether cloud computing is or could be used for a given activity, and determine the appropriate assurance level required for it.

Level 0	No Sovereignty – The minimal requirements of level 1 are not met
Level 1	Jurisdictional Sovereignty – i.e., the cloud computing service provider is established in the EU, customer data must remain in the EU unless allowed otherwise, but direct subcontractors for operational and technical assistance are located outside of the EU.
Level 2	Data Sovereignty – i.e., subcontractors must be established in the EU, holding of at least the assurance level "substantial" under the EUCC, no reliance on the data to fine-tune any AI system operated by a third country or legal entity in that third country.
Level 3	Digital Resilience – i.e., the personnel, including the personnel of the subcontractors, which are involved in the provision of the audited service are EU citizens and where appropriate, the personnel must also have the necessary national security clearance.
Level 4	Full Digital Sovereignty – software supply chain requires effective control over design and evolution of components not merely source code audits and remote-feature blocking, no possibility for public entities to waive requirements.

(names of the levels are provided on the basis of the existing Cloud Sovereignty Framework for illustration purposes; no labels have been given in CADA)

CADA already sets out some examples of assurance levels: national security, internal security, external border management, defence, justice or law enforcement must be at least level 2.

Public procurements must also include as part of the quality criteria (*critères d'attribution du marché*) the tenderer's contribution to the development of a European cloud and AI ecosystem (e.g., integration of EU technology and hardware designed or manufactured in the EU) to the extent linked to the subject matter of the contract and remains a non-decisive element in the award of the contract.

NIS2 entities are also allowed to – i.e., encouraged – to make use of the certification scheme in their risk assessments, with the Commission tasked with publishing guidance and methodology to that end.

CADA also establishes a EuroCloud Federation, open to public entities on a voluntary basis, but subject to a fee paid to the European Commission. Membership to the federation enables the sharing of and joint procurement of data centre and cloud services. The proposal targets specifically 'idle' cloud resources not being actively used.

Key takeaways

CADA is the most operationally direct expression of the EU's shift towards "open strategic autonomy" in the digital sector. For public bodies, it introduces a structured sovereignty classification regime that will reshape how cloud and AI services are tendered, awarded, and governed. For providers – especially those headquartered outside the EU – it signals a market that is actively designing competitive advantage around origin, supply chain transparency, and infrastructure location. This comes at a time where concrete initiatives are also relayed to the retail sector, such as the launch of EuroOffice in early June as a sovereign alternative to an office suite.

Whether or not CADA passes in its current form, it confirms a trend for the upcoming decade of EU digital procurement.