POSITION PAPER
CLOUD AND AI DEVELOPMENT ACT (CADA)

COM (2026)-502 Final & Interinstitutional Procedure Number 2026/0138 (COD)

Towards an Open, Proportionate and Competitive European Digital Sovereignty Framework

September 2026

EXECUTIVE SUMMARY

AmCham Italy shares the European Union's (EU) objective of strengthening capacity, resilience and security in the Cloud and Artificial Intelligence sectors. However, we wish to stress that, as currently drafted, the CADA risks **confusing "Digital Sovereignty" with "Provider Nationality"**, rather than with effective, verifiable and *auditable* control over data, services and operational continuity.

An approach based on origin criteria, rigid localisation and restrictions on trusted third-country providers could lead to reduced competition, higher costs for public administrations, a general slowdown of the digital transformation and substantial limitations on access to the most advanced cybersecurity and AI technologies.

For AmCham Italy, the CADA should pursue an **Open Sovereignty** model: sovereignty understood as the customer's/end user's ability to exercise control and as autonomy of choice, not as the closing-off of markets. US companies investing in infrastructure, skills, research and partnerships in Europe make a decisive contribution to Europe's digital capacity and must be able to compete on the basis of proportionate technical, operational and security requirements.

In light of these considerations, the current text needs to be reoriented towards **risk- and outcome-based, non-discriminatory** criteria, consistent with the Single Market, with the international commitments undertaken by the EU and with the need to attract private investment in Data Centres and AI capacity across the Member States.

DIGITAL SOVEREIGNTY: VERIFIABLE CONTROL, NOT NATIONALITY

The key issue concerns the design of the four Union Assurance Levels. The framework envisaged by the CADA tends to become progressively more restrictive not only in terms of what providers must demonstrate, but also in terms of **who they must be**. This approach risks producing exclusions based on corporate origin rather than on technical and operational evidence.

Sovereignty should be measured through verifiable tools: encryption with customer-managed keys, *confidential computing*, segregation of environments, access controls, independent audits, *disaster recovery*, continuity plans and migration options. These measures allow Administrations to retain control over their data without giving up the best available technologies.

In particular, the most sensitive public workloads, including Defence, National Security and Critical Infrastructure, are precisely those that require the most advanced capabilities in AI, *threat intelligence*, threat detection and incident response. Excluding or limiting trusted global providers may weaken, rather than strengthen, Europe's Security posture.

Company Details
Via Cesare Cantù, 1
20123 - Milano (MI)
VAT No. 01151000153

Contacts
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it

COMPETITIVENESS, PUBLIC COSTS AND INVESTMENT

Narrowing the number of eligible providers would result in less competitive pressure and, consequently, higher costs for the Public Administration and weaker incentives to adopt innovative practices and tools. Moreover, the proposal does not appear to be accompanied by a sufficiently thorough analysis of its effects on national budgets, compliance costs and supply chains. There is also a clear tension between the European objective of attracting private investment in capacity & data centres and a framework that essentially limits access to public demand for precisely those *global players* most prepared and willing to invest across the different EU jurisdictions at this historic moment, in view of the intense technological expansion under way in Europe's socio-economic landscape. Regulatory predictability and non-discriminatory market access are essential conditions for mobilising capital, skills and infrastructure capacity.

OPERATIONAL RESILIENCE AND NATIONAL SECURITY

If the concern relates to possible disruptions in adverse geopolitical scenarios, the most proportionate response is not the pre-emptive exclusion of providers, but the establishment of an operational resilience framework. Multi-cloud architectures, exit plans, backups, contractual continuity commitments, *service level agreements*, *escrows* and zero-access controls can mitigate specific risks while preserving individual end customers' freedom of choice.

Data localisation is only one of the elements contributing to digital security. Effective resilience stems from the combination of advanced technological measures, risk management capabilities, operational continuity and access to the best available expertise. For this reason, an approach based solely on localisation or provider-origin criteria risks failing to fully capture the factors that determine the security and reliability of cloud services.

SUBSIDIARITY, LEGAL CERTAINTY AND THE SINGLE MARKET

The CADA assigns the European Commission a very far-reaching role in defining the *risk assessment* methodology and in the possible review of national assessments. Member States, however, are best placed to assess the sensitivity of their own data, public functions and national security needs. European coordination is therefore necessary, with a clear definition of the competences assigned to EU bodies and to individual national governments.

At the same time, the lack of precise definitions must not be allowed to generate fragmentation. The notion of "public order" should be confined to genuinely critical cases, preventing ordinary Public Administration functions from being automatically drawn towards more restrictive levels. Clear criteria, common thresholds, a transparent methodology and full involvement of the co-legislators are needed.

Company Details
Via Cesare Cantù, 1
20123 - Milano (MI)
VAT No. 01151000153

Contacts
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it

TRUSTED THIRD COUNTRIES AND THE TRANSATLANTIC PARTNERSHIP

The mechanism for recognising associated third countries must therefore be workable, timely and non-discriminatory. Democratic, liberal and trusted partners such as the United States of America are an essential and integral part of the European technology ecosystem. A model in which non-EU providers are structurally confined to the lower *assurance* levels, unless the Commission takes a discretionary decision with no time limit, will create greater uncertainty and a possible deterioration of Foreign Direct Investment (FDI) in the medium to long term.

CADA AND PUBLIC PROCUREMENT ACT: THE NEED FOR SYSTEMIC CONSISTENCY

A further consideration concerns the need to ensure full consistency between the CADA framework and the proposed Regulation on public procurement and concessions, the so-called Public Procurement Act, presented by the European Commission on 9 September 2026. The two texts, currently being negotiated in parallel, affect the same scope of public demand for cloud and artificial intelligence services: the CADA through the four Union Assurance Levels, the Public Procurement Act through a horizontal framework of European preference and criteria on quality, security, supply-chain resilience and sovereignty.

AmCham Italy considers it essential to prevent this overlap from producing a cumulative double filter on the same tender procedure, with the effect of further narrowing the pool of eligible providers beyond what is necessary and proportionate to the actual sensitivity of the data and functions concerned. In this respect, we welcome the fact that the public procurement proposal does not provide for an automatic and generalised exclusion of third-country providers and expressly preserves access for operators covered by the WTO Government Procurement Agreement (GPA) and by the trade agreements concluded by the European Union. We therefore hope that the same principle of safeguarding international commitments will be recognised explicitly and symmetrically in the CADA as well, so as to ensure legal certainty for operators, predictability for contracting authorities and full consistency of the Union's regulatory action. Finally, we recommend that the two legislative processes be accompanied by an explicit clarification of their respective scopes of application and of the relationship between the two sets of rules, avoiding duplicate compliance burdens and ensuring that the overall requirements remain calibrated on objective, verifiable and proportionate criteria.

RECOMMENDATIONS AND CONCLUSIONS

In light of the critical issues highlighted, AmCham Italy therefore considers it appropriate, with regard to the CADA, to:

- **Adopt a proportionate, risk-based approach**, ensuring that sovereignty requirements are calibrated to the actual sensitivity of the data and activities concerned, and avoiding the application of overly restrictive criteria to services and functions that do not present particular critical profiles.

- **Recognise equivalent security measures and operational safeguards,** acknowledging that digital sovereignty can be effectively ensured through verifiable technical, organisational and contractual controls capable of guaranteeing data protection, service continuity and operational resilience.

- **Avoid protectionist or discriminatory criteria**, replacing origin-based requirements with demonstrable obligations of security, resilience, interoperability and effective data control.

Company Details
Via Cesare Cantù, 1
20123 - Milano (MI)
VAT No. 01151000153

Contacts
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it

- **Make the recognition of trusted partners workable**, providing for clear timelines, objective criteria and a model consistent with the GPA/FTA agreements and with the European Union's international trade commitments.

- **Limit the extension to the private sector**, making any possible extension to NIS2 sectors subject to an impact assessment, stakeholder consultation and the ordinary legislative procedure.

- **Ensure balanced governance and legal certainty,** defining the *risk assessment* methodology in primary legislation and carefully limiting the Commission's *override* powers to specific, reasoned and proportionate cases.

The CADA can represent an important step towards strengthening Europe's digital capacity, but only if built on openness, proportionality and competition. Europe needs more investment, more integration, more security and more access to advanced technologies, not a framework that reduces the choice available to Administrations and weakens the innovation ecosystem.

From this perspective, **AmCham Italy hopes that the legislative debate on the CADA will lead to a regulatory framework capable of effectively reconciling the European Union's objectives of security, resilience and strategic autonomy** with the principles of openness, competitiveness and innovation that have historically characterised the Single Market. This requires an approach based on objective and proportionate criteria that recognise providers' actual ability to guarantee data protection, operational continuity, infrastructure resilience, process transparency and service reliability. In this context, the assessment of sovereignty requirements should be based on concrete and verifiable safeguards, **avoiding mechanisms that could lead to generalised restrictions** based solely on the corporate or geographical origin of operators. Such an approach would strengthen the security and competitiveness of the European digital ecosystem, while preserving the integrity of the EU's economic area, its ability to attract international investment and the strategic value of the precious Transatlantic Partnership.

Company Details
Via Cesare Cantù, 1
20123 - Milano (MI)
VAT No. 01151000153

Contacts
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it