GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# POSITION PAPER: CLOUD & AI DEVELOPMENT ACT

*PRESERVING CROSS-BORDER DIGITAL ACCESS ACROSS ALL EU SECTORS*

The Global Data Alliance (GDA)[1] is pleased to offer the following position paper on the European Commission's Cloud and AI Development Act proposal.

The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA members depend on cross-border access to cloud and network infrastructure, digital tools, and information to innovate, operate, and create jobs across the EU. GDA members are active across the agriculture, automotive, aviation, energy, finance, health, hospitality, manufacturing, media, software, telecommunications, transportation, and other sectors in the EU.

## Executive Summary

The GDA supports the Commission's objectives of: (1) expanding sustainable data centre capacity, (2) accelerating artificial intelligence (AI) adoption in strategic sectors, (3) investing in skills and research, and (4) reducing permitting barriers. We also share the Commission's underlying concerns about operational continuity and exposure to extraterritorial legal measures, particularly in economies that do not offer robust legal protections for core human rights and property rights of importance to citizens and stakeholders in the EU and in allied economies.

GDA members rely on global cloud and network infrastructure and digital tools to serve European customers, employ European workers, advance European innovation, and meet European regulatory obligations. Our concern with CADA is focused on whether cross-sector enterprises active across the EU will retain access to the globally integrated digital tools on which their operations, resilience, and regulatory compliance depend.

GDA's view is that "digital sovereignty" is best understood as the ability to build a digital ecosystem grounded in four pillars: **capability, collaboration, resilience, and trust.**[2] Measured against those pillars, several elements of CADA as proposed would work against the objectives they are intended to serve. Criteria keyed to corporate ownership, nationality, or headquarters location — rather than to demonstrated security performance — narrow the range of providers and architectures available to European customers, concentrate rather than distribute operational risk, and impede the cross-border data flows and systematic redundancies on which capability, resilience, and trust all depend. Ownership is not the same as control, and origin is not a reliable proxy for security.

Independent modelling underscores what is at risk when sovereignty measures move from performance-, accountability-, and assurance-based criteria to broad origin-based restrictions. For example, Oxford Economics, modelling five levels of AI sovereignty restrictiveness across the Asia-Pacific, found that costs

[1] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see https://www.globaldataalliance.org

[2] Global Data Alliance, Promoting Digital Sovereignty: Building Capability, Collaboration, Resilience, and Trust into Digital Ecosystems (2026), available at https://globaldataalliance.org.

and risks rise non-linearly when origin-based restrictions are imposed in place of functional performance-based criteria. At the most restrictive levels, firm-level AI adoption in Japan would fall from a projected 20.3% to 3.4% by 2035, with total opportunity costs exceeding US$58 billion (1.4% of 2035 GDP); in Singapore, adoption would fall from 43.8% to 9.6%, at an opportunity cost of 3.2% of 2035 GDP.[3] The impact of strict sovereignty measures – higher costs, slower diffusion, lower productivity – would be similar in the EU.

## Summary Recommendations

The GDA respectfully recommends that co-legislators:

- Ground assurance criteria in demonstrated functional performance metrics rather than corporate origin, nationality, or headquarters location or personnel citizenship mandates;
- Consider the need for investment and legal certainty
- Remove localisation requirements that degrade cybersecurity and operational resilience;
- Recognise encryption, key custody, and access-management architectures in lieu of origin-based mandates;
- Refrain from extending the framework to finance, insurance, health, and other regulated sectors – by deleting Article 31;
- Make "Union added value" criteria optional and delete the hardware-origin criterion in Article 32(3)(d);
- Replace the "associated third country" model with a more open framework.

## Discussion

### 1. Ground assurance criteria in performance – not origin

Under Annex II, assurance levels 3 and 4 exclude providers subject to third-country control — at Level 4, with no recognition pathway at all.[4] This conflates security with corporate origin and undermines the role of technical, legal, and organisational safeguards. A non-EU-headquartered provider operating EU data centres under EU law-governed contracts, with demonstrable technical controls, presents a materially different risk profile from a provider lacking such strong controls and protections. Favoring the latter over the former would restrict market access while weakening privacy and security outcomes.

An EU (or foreign) bank, insurer, or other manufacturer or service provider that has invested time and resources in particular network or software environments may be deemed ineligible for workloads that it has long supported, not because of any identified security deficiency but because of its provider's corporate structure. The same logic penalises European companies that succeed internationally: a European provider that expands globally, takes non-EU investment, or relies on international supply chains for hardware, software, or open-source components may itself struggle to qualify.

### 2. Consider the need for legal and investment certainty

Article 16(2) permits the Commission to amend Annex II criteria by delegated act, with a mandatory review every 18 months. Many EU (and foreign) entities will bear the cost of that instability. Banking, clinical trial, manufacturing, and grid-management systems operate on multi-year horizons that are difficult to reconcile

[3]Oxford Economics for the AI Adoption Initiative, The Economics of Sovereign AI: Balancing Autonomy, Innovation, and Growth in the Asia-Pacific (May 2026), Figures 3, 24 and 25.
[4]European Commission, Proposal for a Cloud and AI Development Act (COM(2026) 502), Annex II and Annex III.

with eligibility criteria that may materially change every 18 months. Companies would face challenges committing to long-term deployments if the underlying service may become ineligible before completion.

## 3. Remove disproportionate localisation mandates

CADA requires at Level 1 that certain data sets remain exclusively within the Union unless the public sector body explicitly requires otherwise, with audit criterion C at Levels 2 to 4 requiring evidence, including data-flow diagrams, that data does not leave the Union. Localisation of this kind reduces resilience by limiting the ability to distribute or replicate workloads across jurisdictions. Organisations whose infrastructure is confined to a single country have markedly fewer disaster-recovery options than those operating geographically distributed, multi-country architectures.

Furthermore, the telemetry and metadata requirements could directly degrade the cybersecurity posture of the services they are meant to protect. Modern security operations depend on cross-border flows and cross-border cloud access. Security operations centres rotate active monitoring across time zones. Threat detection depends on correlating signals across global datasets (e.g, so that a ransomware variant, exploited vulnerability, or malware signature first observed in one region can allow for real-time updates of protection protocols). Forensic cybersecurity teams are geographically dispersed, including outside the EU. The Commission should avoid mandates that cut European customers off from real-time global threat intelligence and that slow incident response: Localisation mandates create unnecessary data silos, impede real-time cyber awareness, and undermine cross-border collaboration on detection and response.[5]

The GDA recommends replacing CADA's data localisation requirements with governance-based controls to avoid disabling the security capabilities on which European customers rely.

## 4. Leverage encryption controls – instead of origin-based restrictions

CADA should recognise technical safeguards as meaningful sovereignty guarantees rather than treating corporate control as the only relevant criterion. Customer-managed encryption architectures, such as Bring Your Own Key and Keep Your Own Key models, provide an auditable, verifiable guarantee that operates independently of a provider's corporate structure: where decryption keys are held exclusively by the customer or by a customer-designated key management service established in the EU, the provider cannot produce readable data in response to a foreign compulsion order. That is precisely the outcome CADA seeks, achieved through architecture rather than ownership tests. Its omission from the Level 3 and 4 criteria is a significant design gap.

The GDA accordingly recommends that co-legislators recognise encryption, key custody, and access-management architectures as qualifying safeguards at every assurance level.

## 5. Remove Article 31 and do not extend the framework to the private sector

CADA's formal scope is public procurement. However, Article 31 would potentially extend its reach deep into the private marketplace, producing significant unintended disruption. Article 31 envisions NIS2-regulated private-sector entities – in energy, transport, health, financial services, and digital infrastructure – applying the same sovereignty risk assessment framework. Article 31 also empowers the Commission to make that application mandatory by delegated act. Recital 66 acknowledges directly that public procurement requirements of this kind tend to be mirrored by private-sector entities in regulated industries.[6] Once the Commission publishes methodology guidance, that guidance becomes the de facto benchmark against which supervisors and counterparties judge voluntary assessments. By the time any delegated act is adopted,

[5]Global Data Alliance, Submission for the 2026 National Trade Estimate Report (Oct. 30, 2025), Box 3 (Cross-Border Data Policy and Cybersecurity).
[6]CADA, Article 31 and Recital 66, which acknowledges that public procurement requirements of this kind "tend to be mirrored" by private-sector entities operating in regulated industries.

mandatory application would formalise an established market expectation rather than create a new one. We outline below several of the unintended consequences across sectors.

***Financial services and insurance***

Financial institutions depend on cross-border data movement for regulatory functions.[7] Fraud detection, sanctions screening, and anti-money-laundering compliance require real-time comparison of transactions against global reference data; confining data within a single jurisdiction narrows the reference set and measurably weakens detection. Group risk aggregation – consolidated supervision, capital adequacy calculation, stress testing, and the ICT risk registers required under DORA –depends on consolidating data across entities inside and outside the EU. Payments depend on global processing infrastructure. For example, domestic routing mandates, such as Vietnam's requirement that domestic card-present transactions be routed through a state-owned national switch, limit competition without a corresponding security benefit.[8]

In insurance, actuarial modelling requires datasets large enough to build credible period and cohort life tables; catastrophe and reinsurance pricing depends on globally pooled loss experience; and claims verification depends on cross-referencing international databases, which after a natural catastrophe is what allows payouts to reach affected policyholders in days rather than months. Restrictions on cross-border health and financial data transfers reduce the range of insurance products available to customers and increase cost.

The Republic of Korea offers a cautionary case study. Localisation and network segregation requirements prevent Korean subsidiaries of global financial institutions from drawing on group IT and cybersecurity expertise, and have inhibited adoption of SaaS-delivered and AI-enhanced cybersecurity tools. Reinsurers remain constrained in the ability to process policyholder data. The measurable results are a larger attack surface, more potential points of failure, and reduced cross-border threat visibility – the opposite of the resilience the measures were intended to deliver.[9]

The EU already has a purpose-built framework for financial-sector ICT resilience in DORA, supplemented by NIS2 and sectoral prudential rules. Layering CADA sovereignty criteria onto that architecture would produce overlapping regimes, inconsistent supervisory expectations, and higher compliance costs without a demonstrated security gain.

***Healthcare, biopharmaceuticals, and medical devices***

Few sectors are as dependent on cross-border data as health and life sciences.[10] In clinical trials, data flows are required to identify and establish trial sites, recruit and monitor participants, and prepare submissions for each national regulator that may approve the medicine. Pharmacovigilance obligations – adverse event reporting, site inspections, and post-authorisation safety studies – are inherently transnational. New treatment discovery depends on cross-border analytics that can shorten candidate identification from years to months, drawing on clinical, genomic, registry, and real-world evidence datasets. Demographic representativeness – critical to ensuring that a therapy is safe and effective across populations – depends on pooling data across regions; localisation narrows the evidence base and can bias results.

In medical technology, device telemetry crossing transnational networks is what allows manufacturers to monitor the safety and efficacy of implanted and connected devices, to conduct health economic analysis of patient outcomes, and to engineer improvements. Remote diagnostics and cross-border referral depend on

[7]Global Data Alliance, Cross-Border Data Transfers & Finance (2022).
[8]Global Data Alliance, 2026 NTE Submission at 48 (Viet Nam: State Bank of Viet Nam Circular 18/2024/TT-NHNN requiring domestic card-present transactions to be routed through NAPAS).
[9]Global Data Alliance, 2026 NTE Submission at 27 (Republic of Korea: network segregation and localisation measures; Financial Supervisory Service interpretation treating global support as a violation of network segregation rules; continuing inability of reinsurers to transfer policyholder data).
[10]Global Data Alliance, Cross-Border Data Transfers & Healthcare (2022); Global Data Alliance, Biopharmaceutical R&D (2022); 2026 NTE Submission at 11 (Box 4).

comparing patient data against larger transnational datasets, supporting more precise diagnoses and avoiding unnecessary treatment.

Health is expressly among the NIS2 sectors named in Article 31, and health workloads are among those most likely to be assessed as requiring higher assurance levels. The practical effect would be to restrict which platforms European hospitals, trial sponsors, registries, and device manufacturers may use for EU-based activity — with consequences for the speed at which European patients gain access to new therapies, and for Europe's attractiveness as a locus of health research, development, and delivery.

The GDA accordingly recommends that co-legislators delete Article 31, so that CADA criteria are not extended – by supervisory expectation or by delegated act – to private-sector entities and their commercial contracts. The GDA also recommends that co-legislators confirm that DORA, NIS2, the GDPR, the AI Act, and applicable sectoral rules remain the operative frameworks for private-sector ICT risk management, with CADA limited to clearly defined sensitive public sector use cases.

## 6. Make "Union Added Value" Award Criteria Optional; Remove Hardware-Origin Criteria

Article 32 would require contracting authorities to apply "Union added value" non-price award criteria in procurement of innovative cloud and AI services. Given the cross-sectoral impact of such procurement decisions on GDA members, the GDA recommends that this be made optional: while authorities should be permitted to weigh ecosystem contribution where the criteria are objective, transparent, proportionate, and linked to the subject matter of the contract, these "Union added value" criteria should not carry undue weight.

The only safeguard against Article 32 operating as a *de facto* origin preference is the requirement that such criteria remain "ancillary and not decisive." That constraint is qualitative and unenforceable in practice. It sets no numerical ceiling and creates no route to challenge an award where the criteria proved outcome-determinative. A criterion nominally worth 15 of 120 points may be decisive whenever the remaining criteria produce a close result among leading tenderers. The GDA therefore recommends that the "Union added value" criteria be explicitly characterized as "optional," and that a review mechanism be established to allow tenderers to challenge awards where the criteria were not actually "ancillary."

Article 32(3)(d) warrants deletion outright. Requiring authorities to assess whether critical computing, storage, and networking hardware was designed or manufactured in the Union is an industrial preference embedded in a security instrument. The geographic origin of a chip or server does not determine the security of the service running on it, and given the distribution and interdependence of modern hardware supply chains, the criterion would be close to unverifiable in practice. It should be replaced with criteria that have a genuine functional, performance, or security rationale.

For the same reason, Member States should be able to rely on Article 30(4) derogations without onerous evidentiary requirements where no certified service at the required level exists, or where certified alternatives are technically inadequate for the use case.

## 7. Replace the "associated third country" model with a more open framework

Article 18 would permit third-country-controlled providers to reach Level 3 only where their home country is designated an "associated third country." The GDA supports cooperation with trusted partners and agrees that continuity of service, lawful access safeguards, open markets, and reciprocity are the right considerations. But the criteria as drafted are too rigid, and risk excluding longstanding partners on whom Europe's cloud, AI, cybersecurity, and semiconductor supply chains materially depend. Business organisations in Australia, Canada, Japan, and the United States – economies with which the EU maintains close regulatory and security cooperation – have already voiced concern about exclusion from made-in-Europe initiatives. Europe's resilience depends as much on trusted partnerships as on domestic capability;

treating every third-country relationship as a vulnerability forfeits the collaboration pillar of sovereignty in pursuit of the others.

Designation must also be predictable. The Commission should give reasons for any designation, refusal, suspension, or withdrawal, identify the evidence relied upon, and allow structured dialogue before market access consequences take effect. CADA should also include transition and remediation rules: where a country loses designation, providers with ongoing contracts need a realistic phase-out period, and their customers need continuity safeguards and a route to remediate specific concerns. Abrupt loss of eligibility mid-contract transfers operational risk directly onto the hospital, utility, or bank that relied on the service — the precise harm CADA is meant to prevent. Early warning and consultation mechanisms between trading partners, of the kind the GDA has long advocated, would allow such risks to be managed cooperatively rather than through unilateral exclusion.[11]

## Conclusion

The GDA supports the Commission's objectives of greater capacity, stronger resilience, and reduced exposure to disruption. These objectives are best achieved by building capability up rather than shutting partners out – through investment in infrastructure, skills, and innovation; collaboration with like-minded partners; resilience built on diversity, redundancy, and interoperable standards; and trust grounded in transparent governance and verifiable technical safeguards. Origin-based restrictions reduce the choice and architectural diversity from which resilience is actually built, and impose their heaviest costs on the European citizens and stakeholders that CADA is intended to serve.

A CADA that is risk-based, technology-neutral, and grounded in functional performance metrics can strengthen Europe's digital sovereignty while keeping European industry connected to the global networks on which its competitiveness depends. The GDA and its members stand ready to work with co-legislators, the Commission, and Member States toward that outcome.

[11]Global Data Alliance, Cross-Border Data Policy Principles (2021).