

Our position

Cloud and AI Development Act



AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €4 trillion in 2023, directly supports more than 4.6 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Table of content

Summary of recommendations	3
Executive summary	6
Introduction	7
Areas of support	7
Pillar 1: research, development and innovation (R&D&I)	7
Pillar 2: data centre capacity and infrastructure	8
Areas of improvement	9
Trust without origin-based market access barriers	9
Recommendations for the sovereignty framework	9
1. Scope	10
2. Private-sector spillover	12
3. Financial links	13
4. Union cloud computing sovereignty framework and assurance levels	14
5. Speed and legal certainty	16
6. Procurement and EU-added value	16
Conclusion	17

Summary of recommendations

Priority area	Subtopic	Suggestions
Research, development and innovation	Funding and access to compute	Ensure stable, coordinated EU funding. Support demand-side investment and digital skills. Maintain technology-neutral access to compute. Keep initiatives open to trusted international partnerships.
Data centre capacity and infrastructure	Investment and permitting	Accelerate permitting, grid connections and enabling infrastructure. Avoid overly prescriptive geographical planning. Ensure predictable energy costs. Apply broad, technology-neutral eligibility for strategic projects.
Annex II	Risk-based approach	Base sovereignty requirements on demonstrable risk, control and operational resilience rather than ownership, nationality or corporate domicile. Apply requirements proportionately across assurance levels and workload types.
	Establishment, control and personnel	Require EU establishment only where necessary. Replace ownership-based restrictions with objective risk assessments. Use residency and subjection to EU law rather than citizenship requirements.
	Customer vs operational data	Distinguish customer production data from telemetry, metadata and other operational data. Limit localisation requirements to data presenting genuine sovereignty risks and preserve global cybersecurity capabilities.
Scope	Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS)	Differentiate requirements according to service model, workload criticality and data sensitivity. Apply lighter requirements to lower-risk SaaS and PaaS services and reserve higher assurance levels for genuinely critical workloads.

Priority area	Subtopic	Suggestions
	Definition of cloud services	Limit CADA to genuine cloud computing services meeting the NIS2 definition and avoid capturing traditional hosted or cloud-enabled solutions that do not involve scalable and elastic pooled resources.
	Data Act and AI Act	Align cloud-related definitions with the Data Act and avoid introducing unnecessary new AI concepts. Replace references to 'AI agents' with existing AI Act terminology where appropriate.
Private-sector spillover	Article 31 / NIS2 entities	Keep the sovereignty framework focused on public-sector procurement and remove Article 31 to avoid duplicating requirements already addressed through DORA, NIS2 and other sector-specific frameworks.
Financial links	Meaning of 'financial links'	Clarify that ordinary banking and financial relationships do not constitute third-country control, avoiding unintended consequences for financial institutions and technology providers.
Union cloud computing sovereignty framework and assurance levels	Third-country equivalence	Preserve a workable equivalence pathway and ensure criteria are proportionate, clearly defined and based on demonstrated risks. Use reciprocity restrictions only as a narrow backstop against verified discrimination.
	Software supply chain and certification	Apply software requirements only to security-critical components and align them with recognised standards. Recognise equivalent international cybersecurity certifications until the European Cybersecurity Certification Scheme becomes operational.
	Data localisation and subcontracting	Avoid blanket EU localisation of telemetry and metadata. Preserve global cybersecurity capabilities. Limit obligations to subcontractors that materially contribute to the covered service.

Priority area	Subtopic	Suggestions
Speed and legal certainty	Audit and revalidation	Replace annual revalidation with continuous monitoring and reassessment following material changes, while recognising existing compliance mechanisms where they address equivalent risks.
Procurement and EU-added value	Competition and interoperability	Promote interoperable and multi-cloud environments. Preserve supplier choice and avoid procurement criteria that unnecessarily restrict competition. Maintain proportionate derogations for emergency and operational necessity.

Executive summary

The success of the Cloud and AI Development Act (CADA) will depend on whether its sovereignty framework strengthens Europe's resilience and competitiveness without restricting access to the technologies, providers and operating models needed to support the bloc's digital transformation. As currently envisaged, several elements of CADA introduce origin-based restrictions that are not necessarily linked to genuine sovereignty, security or resilience risks. These measures could reduce competition, increase costs and slow cloud and AI adoption – ultimately working against CADA's underlying objectives.

AmCham EU supports efforts to strengthen Europe's cloud and AI ecosystem, accelerate public sector adoption, expand research and innovation and improve resilience across the digital economy. CADA can contribute to these goals, but only if sovereignty requirements are based on demonstrable risks and remain proportionate, technology-neutral and open to effective competition.

To ensure CADA achieves its objectives, the co-legislators should:

- Base sovereignty requirements on demonstrable control and risk rather than ownership, nationality or corporate domicile.
- Apply a proportionate, risk-based approach across assurance levels, cloud service models and workload types.
- Ensure sovereignty requirements strengthen rather than undermine cybersecurity, operational resilience and service continuity.
- Maintain a technology-neutral framework that recognises global operating models and existing security and compliance mechanisms.
- Keep CADA focused on the public sector and avoid duplicating requirements already addressed through DORA, NIS2 and other sector-specific frameworks.
- Promote competition, interoperability and supplier choice while avoiding measures that reinforce vendor lock-in.
- Provide legal certainty through a workable equivalence framework, proportionate compliance requirements and efficient recognition procedures.

A sovereignty framework built on objective, risk-based criteria will better support Europe's competitiveness, resilience and digital transformation than one based on origin, ownership or nationality.

Introduction

American companies are woven into the fabric of the EU's digital economy, delivering cloud computing, AI and software services to millions of European businesses, public-sector bodies and citizens. The Cloud and AI Development Act aims to strengthen the resilience and competitiveness of this ecosystem, and its impact will extend well beyond cloud providers and infrastructure operators. Many industries increasingly rely on cloud services to conduct research, develop innovative products, manage global operations and deliver services to customers. Across sectors, AmCham EU has a strong interest in ensuring that CADA supports innovation, security and competition while achieving legitimate sovereignty objectives.

Building economic resilience, fostering homegrown European technology companies and scaling a competitive domestic digital industrial base are all worthy objectives. The concern with CADA is not the ambition itself, but whether the Act pursues its goals through discriminatory exclusion, origin-based tests or unworkable requirements.

In particular, CADA's assurance level framework introduces structural requirements, including establishment mandates, ownership control tests and citizenship obligations, that go substantially beyond existing EU law, including the GDPR. This framework risks fragmenting the transatlantic digital economy for both technology providers and the businesses that rely on their services. We urge co-legislators to ensure alignment and coherence between CADA, the Industrial Accelerator Act and the Public Procurement Act in order to avoid regulatory duplication and conflicting compliance obligations. Any expansion of CADA beyond public procurement should equally recognise existing sectoral frameworks, including DORA and NIS2, that already address cybersecurity and operational resilience, third-party risk and dependency risks.

This paper first outlines areas of the CADA proposal where we support the Commission's approach and areas where we believe further refinement would improve the initiative's overarching objective, proportionality and legal certainty.

Areas of support

Pillar 1: research, development and innovation (R&D&I)

CADA forms part of a broader Tech Sovereignty Package that includes supply-side ambitions – Cloud and AI Leadership Initiatives, grand challenges, and R&D&I objectives. A more capable and diversified European cloud and AI ecosystem benefits all market participants, including global providers with large-scale European investments and operations.

For these initiatives to deliver, co-legislators should ensure:

- **Stable and predictable funding through Union programmes** (including the European Regional Development Fund, the European Competitiveness Fund and the upcoming Multiannual Financial Framework), with genuine synergies across the Chips Act 2.0, the open-source strategy and national programmes – without fragmentation among these initiatives.
- **Resource-efficient infrastructure solutions:** Union funding should focus on the development, demonstration and scale-up of technology-neutral solutions that improve the combined

energy, water and carbon performance of data centres. Funding should remain open to partnerships across the data centre value chain, including technology and service providers.

- **Demand-side investment alongside supply-side capacity:** stimulating adoption across the economy is as important as building infrastructure. Measures should actively support deployment, digital skills and access to compute – particularly for AI use cases, which are set to grow rapidly in cloud-delivered form.
- **Technology-neutral access to compute** for frontier AI research and public-interest projects, avoiding designs that favour particular architectures or incumbents.
- **Openness to international partnerships:** reinforcing European capabilities should go hand in hand with maintaining openness to trusted partners and global innovation ecosystems, consistent with EU trade commitments.

Pillar 2: data centre capacity and infrastructure

CADA's data centre acceleration zones and data centre strategic projects address a real structural gap. Compute capacity in the EU is insufficient to meet the demands of an AI-intensive economy. AmCham EU supports measures to accelerate build-out, provided they are designed to attract investment from all credible providers – European and international alike.

Recommendations:

- **Treat data centre acceleration as a systemic national administrative goal that extends beyond 'data centre acceleration zones' or 'data centre strategic projects'.** This holistic commitment to administrative efficiency provides the predictability necessary for high-value investment and creates structural efficiencies with positive spillovers into other strategic digital and infrastructure domains.
- **Facilitate the conditions that allow providers to meet demand where it naturally arises.** Data centre deployment is driven by multiple factors such as market demand, customer proximity, water, grid/energy viability and local receptiveness rather than centralised geographical planning. The top-down approach to distribution risks decoupling investment from economic reality.
- **Simplify permitting, grid access and enabling infrastructure.** Faster and fully digitalised approval processes are essential. Outdated grid infrastructure, long connection queues, energy and resource constraints and complex permitting regimes are the primary obstacles to investment; CADA should address these directly rather than leaving them to Member State discretion. For example, acceleration zones should integrate grid capacity, connectivity and access to adequate water infrastructure.
- **Address energy competitiveness.** The viability of data centre investment depends on predictable, competitively priced clean and renewable electricity and proportionate grid fees over the asset's full operating lifetime. Regulatory unpredictability on energy costs is a significant deterrent to long-term capital commitment.
- **Build sustainability requirements on existing workstreams, such as the EED rating scheme.** Introducing new, divergent Member State measures fragments the investment environment. At the same time, sustainability requirements should remain flexible and take into account and adjust to local conditions.
- **Make the eligibility criteria for data centre strategic project designation broad and technology neutral, with predictable criteria and transparent timelines.** This will enable a wide range of providers to anchor investment in EU infrastructure. Sustainability and innovation criteria should recognise projects that deliver measurable improvements in overall

resource performance, including through advanced cooling, water reuse and treatment, digital resource optimisation or waste-heat recovery.

Areas of improvement

Trust without origin-based market access barriers

Building greater trust in cloud and AI services is necessary to accelerate public sector adoption. Achieving that objective, however, requires the law to rely on verifiable, technology-neutral and operationally meaningful criteria – not on the nationality or geographic origin of the service provider. Sovereignty, in a regulatory sense, should be defined by the degree of control a customer exercises over its own data, systems and operational continuity – not by where a provider's headquarters is located. A framework that conditions market access on a provider's nationality or corporate domicile risks narrowing the field of qualifying vendors in ways that do not track actual sovereignty risk and ultimately work against resilience rather than for it.

The policy debate also needs to distinguish between broad geopolitical concerns and the commercial reality of trusted companies that invest in European infrastructure, employ European workers and comply with EU law. Addressing dependency concerns by excluding firms with that track record may reduce dependency on paper, but it also narrows supplier choice, raises costs, slows deployment and reduces innovation and adoption of innovative technologies.

Notably, the Commission's own impact assessment acknowledges that GDPR enforcement has produced compliance solutions rather than concrete changes in dependency. Yet CADA responds by imposing structural barriers rather than building on the operational and technical safeguards that have proven effective. A GDPR-compliant provider operating EU-located infrastructure, with EU-resident personnel and EU-audited security controls, presents a fundamentally different risk profile from the abstract third-country dependency that CADA's ownership tests are designed to address.

Vendor dependency should instead be assessed through objective market and security metrics, including provider concentration, substitutability, operational resilience, continuity and security safeguards. CADA needs measures that foster an open and interoperable ecosystem, as without genuine choice there can be no credible sovereignty. CADA can complement existing EU initiatives by addressing software licence lock-in, supporting licence portability, non-discriminatory licensing practices and software equivalence across cloud environments.

Where legitimate concerns exist regarding legal conflict, continuity or access, CADA should rely on targeted, objective technical, contractual and operational safeguards rather than blanket exclusions. Auditable technical, contractual and operational controls should be part of the sovereignty conversation – not set aside from it.

Recommendations for the sovereignty framework

We recommend the following amendments to the sovereignty criteria under Annex II:

Place of incorporation: Require EU establishment of the contracting cloud service provider, but not of all subcontractors. Global supply chains should remain permissible where appropriate technical, contractual and operational safeguards are in place.

Third-country control: Replace ownership-based restrictions with objective assessments of operational resilience, continuity, security and substitutability. Sovereignty should be assessed on demonstrable risk rather than corporate structure.

Infrastructure, assets and personnel: Apply requirements proportionately according to workload criticality and the type of data involved. Global support functions should remain permissible where protected by appropriate technical controls.

Data localisation: Distinguish customer production data from operational data such as telemetry and metadata. Localisation requirements should focus on customer production data, while operational data should remain subject to appropriate safeguards.

Personnel requirements: Replace citizenship requirements with criteria based on residency and subjection to EU law, limited to personnel with access to customer production data.

Software supply chain: Adopt a risk-based approach focused on security-critical components and aligned with recognised industry standards. Requirements should not impose de facto restrictions on globally developed software or open-source components.

Outsourcing and subcontracting: Limit restrictions to activities that create genuine sovereignty or security risks and clarify the definitions of outsourcing, sub-outsourcing and subcontracting.

Cybersecurity certification: Recognise internationally accepted cybersecurity certifications (such as ISO/IEC 42001 for AI management systems) until the European Cybersecurity Certification Scheme for Cloud Services (EUCCS) becomes operational.

Audit and compliance: Replace annual revalidation requirements with continuous monitoring and reassessment following material changes, and recognise existing GDPR compliance mechanisms where they address equivalent risks.

The Commission should also provide greater clarity on how the sovereignty criteria apply across different cloud service models and operating environments. Experience with previous cloud sovereignty assessment frameworks has shown that overly rigid scoring methodologies and unclear criteria create legal uncertainty and inconsistent outcomes. Any future assessment methodology should be transparent, proportionate and capable of reflecting overall risk rather than being driven by a single criterion.

1. Scope

1.1. Differentiation between cloud service models and workload criticality

CADA does not sufficiently recognise the range of service delivery models in the EU's cloud market today. As highlighted in Recitals 80-82 of the Data Act, cloud services in Europe include a substantial number of services with a broad range of purposes. These include infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), service delivery models that each have a specific, pre-packaged combination of ICT resources offered by a provider of cloud services. These three fundamental cloud delivery models are further complemented by additional variations, such as Storage as a Service, Database as a Service and now GPU as a Service. Clarifying how CADA's

sovereignty assurance levels apply to the main cloud service delivery models on the market will help reduce some of the ambiguity of the current text.

CADA applies a single definition of 'cloud computing service' across all assurance levels without differentiating between IaaS, PaaS and SaaS. This is problematic because the sovereignty risk profile of these service models differs materially. For example, a SaaS application processing non-sensitive administrative data presents fundamentally different control and access risks than an IaaS offering hosting classified workloads. Indeed, as reflected in the Commission's supporting Impact Assessment, many standard enterprise applications – such as workforce management (payroll, recruitment), inventory, accounting and CRM – are fundamentally non-critical back-office tools that do not control real-time physical operational infrastructure or public safety.

To address these distinct profiles and prevent Single Market fragmentation, the co-legislators should introduce service and application-model differentiation into the assurance framework by permitting a lighter-touch approach for SaaS and PaaS offerings. In practice, this should be achieved by explicitly confirming in the main legal text that SaaS and PaaS offerings do not share the same requirements as IaaS, particularly regarding data localisation mandates. Higher assurance tiers should be strictly reserved for infrastructure-layer services handling operationally critical workloads. Additionally, lighter requirements should apply for non-critical uses of SaaS and PaaS to reflect their lower risk profiles and impact. Establishing this distinction will prevent Single Market fragmentation and accelerate public sector digital transformation, while ensuring European public authorities can access the cloud services best suited to their needs and budgets.

Requirements relating to infrastructure, assets and personnel should be risk-based and reflect the sensitivity of the data involved and the criticality of the service. Certain specialised support functions may require access to global expertise that cannot feasibly be replicated in every jurisdiction. CADA should therefore allow appropriately controlled access by non-EU personnel where necessary to maintain service quality, resilience and security.

1.2. Limited application to genuine cloud computing services

CADA should be understood as regulating cloud computing services that are 'a scalable and elastic pool of shareable computing resources'. It should not aim to regulate all cloud-enabled solutions or applications simply because they are hosted on, rely on, or integrate with cloud infrastructure. CADA incorporates the definition of 'cloud computing service' from Article 6(30) of Directive (EU) 2022/2555 (NIS2), which refers to a scalable and elastic pool of shareable computing resources. Accordingly, services should be assessed on whether they exhibit these core characteristics, rather than whether they are simply hosted on cloud infrastructure. Traditional hosted or 'cloud-enabled' solutions, which operate on a fixed-capacity, dedicated basis without scalable and elastic pooled resources, should not be classified as cloud computing services. This aligns with the actual risk CADA is trying to address. Sovereignty concerns addressed under Annex II (third-country access, service disruption, compelled compliance) are most relevant where infrastructure is pooled across many customers since a compromise at that layer can expose the entire customer base at once. A fixed-capacity, single tenant does not carry such systemic exposure and is closer to traditional dedicated outsourcing which is already sufficiently managed through existing procurement, resilience and data protection requirements.

CADA should clarify that its assurance framework applies strictly to genuine cloud services as defined under NIS2, avoiding the inclusion of traditional hosted solutions. If not, CADA could create multiple

unintended consequences. First, these requirements could divert already scarce audit capacity away from genuinely pooled systemically important services toward lower risk services. Second, it creates legal uncertainty that discourages the public sector adoption that CADA is meant to accelerate. Lastly, it disproportionately burdens smaller hosted-solution providers, which cuts against the SME participation objectives in Article 33.

CADA should also distinguish between customer production data and operational data such as telemetry and metadata. While localisation requirements may be appropriate for sensitive customer data, applying the same requirements to operational data would undermine cybersecurity, incident response and service reliability without delivering corresponding sovereignty benefits.

1.3. Alignment with the Data Act

CADA should not use a different definition of cloud to the Data Act. The Data Act, whose switching and interoperability provisions are cited as an enabler for CADA, relies on a definition of ‘data processing services’, while CADA uses NIS2’s ‘cloud computing service’ definition.

A clearer explanation is needed to justify the distinction, otherwise CADA risks creating two competing and, in certain cases, overlapping, legal definitions for cloud services in Europe, when only one is needed. This runs contrary to the EU’s simplification push.

1.4. Definitions of ‘frontier AI’ and ‘AI agent’ should be reconsidered

The definitions of frontier AI and AI agent are not included in the EU AI Act and will likely have an impact on the AI legislative framework.

- Frontier AI almost always would be ‘GPAI’ under the EU AI Act’s terminology but that connection is not made in CADA. We suggest focusing on the models themselves rather than ‘AI systems built upon such models’.
- The term ‘AI agent’ is extremely hard to define, and it is not clear why it would need to be defined in this law. The term is only used in Article 3(2)(f), Article 4(6). In these instances, we suggest replacing ‘AI agent’ with the term ‘AI systems’. This does not impact the goal of these articles and avoids the need to provide a definition that is complex and should be provided in a different legislative framework. Furthermore, the definition proposed covers all AI, not just GPAI, and does not add much to the AI Act definition of ‘AI system’ besides ‘using tools’. Without a definition for ‘tools’, which will also be elusive, this definition does not add much.

2. Private-sector spillover

CADA appears to go beyond public procurement in one significant respect. In Article 31, it strongly encourages private-sector entities under Annex I of the NIS2 Directive to consider applying sovereignty risk assessments themselves, and grants the Commission substantial delegated powers to go further still – adopting risk mitigation measures and therewith expanding the scope of application to the private sector for those entities where it concludes, ‘duly justified’, that this is required.

This is a substantive extension of the framework’s logic into private markets, going beyond a simple technical suggestion. The EU co-legislators should ensure that private enterprises are not brought into the scope of the Regulation, which is intended to target the public sector. A delegated authority to mandate far-reaching requirements as part of a delegated act rather than the ordinary legislative

process seems disproportionate considering the potential impact. This creates significant legal uncertainty.

There should be no ambiguity as to whether companies operating in sectors of high criticality fall within CADA's scope. NIS2 Annex I entities are additionally concerned regarding the Commission's ability to produce guidance for sovereignty risk assessments that could be applicable or practical across all entities or sectors. Telecommunications, water, credit institutions and healthcare do not share regulatory frameworks and there is no ability for sectors, or their regulators, to input into any Commission guidance.

2.1 Overlap with existing sectoral frameworks

Business continuity and operational resilience amidst geopolitical shocks in regulated private sectors is a real and legitimate concern. The EU has already built dedicated regimes to manage it. These include DORA for ICT and third-party risk in finance, sector-specific resolution and prudential frameworks and NIS2 for critical infrastructure operators.

These regimes are calibrated to the specific risk they address, supervised by authorities with the relevant sectoral expertise and enforced through tools suited to that risk – capital and resilience requirements, incident reporting, resolution planning – rather than by conditioning market access on a vendor's nationality.

Article 31 should therefore be removed from the text. The application of CADA sovereignty risk assessments to Annex I NIS2 entities does not address a regulatory gap. Business continuity, operational resilience and third-party risk are already addressed through sector-specific frameworks, including DORA, NIS2 and other sectoral resilience regimes, which are supervised by competent authorities with the relevant expertise and calibrated to the risks of each sector.

3. Financial links

The financial services sector is concerned that CADA's Audit criterion G(1)(f) could infer that a banking relationship with a cloud, software or AI provider could be deemed as having a level of third-country control over the entity. The Commission should amend the use of the term 'financial links', or clarify this does not relate to a banking relationship, as this could result in significant unintended consequences (Box 1).

A financial institution could be considered to have 'financial links' with a provider in a multitude of circumstances: payment services, commercial banking services, funding rounds, initial public offerings or any mergers and acquisition activity. None of these services constitute any form of third-country control over that provider. Any unintended consequences that could result in debanking should be removed from CADA as this would go against the objectives of the Act.

Box 1 – Examples of implications for financial services

As drafted, CADA could create several direct implications and spillovers for the financial services sector, layering additional requirements on top of the existing DORA framework:

- **Extension of the DORA ICT value-chain assessment:** the existing DORA assessment of ICT third-party value chains would be extended to also examine the ultimate country of control of ICT providers to the financial services industry. This overlaps with existing geopolitical risk assessments and further technology-specific cloud outsourcing guidance produced by the European Central Bank, which includes guidance on evaluating geopolitical risk.
- **Assurance levels 2–4 for financial institutions:** the application of assurance levels to the financial sector could create difficult unintended consequences for financial institutions, who often operate internationally, to implement. For example:
 - Level 4 would require fully European ICT providers across all a financial services provider's activities, including subcontractors of those providers. CADA does not indicate if this would be applied to the financial institution's operations outside of the EU.
 - Level 2 would already require financial institutions to contract only with legal entities established in the EU, raising real questions for current outsourcing arrangements. According to the CADA proposal, a jurisdiction that does not follow the EU's sanctions regime would not meet the assurance criteria 2(g)(iv), therefore removing the ability to use providers from outside of the European Free Trade Association (EFTA).
- **Spillovers from financial market infrastructure (FMI) designation:** where an FMI is designated at level 4, this could have knock-on effects across the wider financial services industry, as the FMI may in turn impose additional requirements on the financial institutions that connect to it. This would impair foreign financial institutions' ability to operate in the EU.
- **Additional audit burden:** any sovereignty measures would need to be externally audited, adding cost and raising questions about the availability of audit services able to meet the resulting demand.

4. Union cloud computing sovereignty framework and assurance levels

4.1. Proportionate and risk-based sovereignty criteria

The criteria linked to third-country control, lawful access, service disruption, telemetry and metadata appear, even at low assurance levels, capable of becoming de facto market access barriers.

The third-country equivalence pathway under Article 18 is a positive and commercially sensible proposal. It creates a route for global vendors to achieve Union assurance level (UAL) 3 recognition. That said, the cumulative criteria, which require simultaneous satisfaction of a GDPR adequacy decision, absence of measures enabling governmental data access conflicting with the EU Data Act, absence of measures compelling service disruption or sanctions compliance, no impediments to state-of-the-art technology provision, maintenance of an open market to EU cloud services and equivalent procurement access for EU providers, raise proportionality concerns.

The requirement that a third country have 'no measures in place' to compel service disruption, for instance, may be read so broadly as to encompass routine regulatory authority that exists in every jurisdiction. The co-legislators should therefore calibrate these criteria carefully and support them

with implementing guidance that provides legal certainty. If retained, reciprocity provisions should operate only as a narrow and exceptional backstop where there is clear and verified discrimination against EU providers and no less restrictive alternative is available. More broadly, restrictions on third-country participation should be based on demonstrated risk rather than a default presumption of exclusion.

In this context, it is noteworthy that the European Data Protection Supervisor (EDPS) has also called for greater legal certainty around Article 18, including clarification of its interaction with GDPR adequacy decisions, the treatment of third-country-controlled providers and the consequences of changes to the adequacy status of a third country. These observations reinforce the need for a clearer, more predictable and legally coherent equivalence framework.¹

Citizenship should not be a sovereignty criterion at UAL 2 and UAL 3. The relevant consideration is whether personnel with access to customer production data are subject to EU law and jurisdiction. CADA should therefore rely on residency and jurisdictional tests rather than citizenship requirements, focusing on those personnel whose roles create genuine sovereignty risks.

Software supply chain requirements should likewise follow a risk-based approach. Requirements relating to software bills of materials, source-code reviews, migration plans and third-country software components should focus on security-critical components and be aligned with recognised industry standards. The framework should avoid creating de facto restrictions on globally developed software or widely used open-source components where no demonstrable risk exists.

The escalation from state-of-the-art cybersecurity standards at UAL 1 to European cybersecurity certification at higher assurance levels is reasonable in principle. However, until the European Cybersecurity Certification Scheme for Cloud Services (EUCS) becomes operational, equivalent international certifications should be recognised as interim compliance pathways in order to avoid legal uncertainty, market fragmentation and unnecessary barriers to adoption.

4.2. Data localisation and operational resilience

The requirement that metadata and telemetry data be exclusively processed and stored within the EU, including by subcontractors, is disproportionate to the risk profile involved, especially for UAL 1.

Modern cloud infrastructure is designed to operate as a seamless, unified entity rather than a collection of isolated regional deployments. At the core of this architecture, systems require highly available and durable data that is globally replicated, accessible and capable of scaling automatically.

An EU silo for telemetry and metadata would undercut critical cybersecurity for European cloud customers, preventing protection at the highest level against emerging cybersecurity threats. The continuous collection and analysis of network telemetry empowers security operations teams to proactively detect network-based threats and hunt for advanced adversaries. This global visibility allows cloud providers to automatically baseline normal behaviour and flag anomalies in real time.

¹ EDPS, opinion 14/2026 on CADA, 29 July 2026, page 11.

This is particularly problematic because CADA defines ‘customer data’ to include not only data input by the customer but also data derived from the customer’s use of the service, including telemetry and metadata (Annex III, Criterion C).

CADA’s UAL 1 mandates that all customer data, including metadata and telemetry data, must remain exclusively localised within the Union. This creates a dangerous blind spot in the global defence network. When threat intelligence is siloed, crucial telemetry data cannot be shared globally to mitigate pressing cybersecurity risks.

The most effective way to defend against large-scale attacks, such as distributed denial-of-service (DDoS) campaigns or zero-day exploits, is to identify threat signatures globally and block malicious traffic as close to the attacker's source as possible. If European telemetry is walled off, the system loses the ability to correlate European traffic patterns with global anomalies. Consequently, malicious traffic must reach European borders before it can be effectively analysed and mitigated, increasing the risk of infrastructure overwhelm.

Requiring full EU localisation of operational telemetry that poses no sovereignty risk imposes enormous technical costs without corresponding security benefits.

Additionally, as currently drafted, the definition of subcontractor captures *any* third party that ‘contributes to the provision and delivery of the service’ under a direct contract, without any threshold for how significant that contribution needs to be. Read literally, this could capture vendors with no substantive connection to the service’s security, resilience or sovereignty profile. That is clearly not the intended target of the CADA framework. Therefore, the co-legislators should refine the text by explicitly specifying that obligations apply to subcontractors involved in the *material* provision of the covered cloud or AI service.

While the possibility of a waiver mechanism is welcome, this should not be the exception but rather the rule. Data localisation mandates of this magnitude should only be imposed in specific circumstances and after a clear cost-benefit analysis.

5. Speed and legal certainty

We support the Commission's goal of strengthening trust and legal certainty to accelerate public sector cloud and AI adoption, but, as drafted, CADA risks introducing administrative complexity that undermines this.

In particular, **criteria based on origin, ownership or nationality – rather than demonstrable risk – could exclude providers with strong technical and operational safeguards, undermining cybersecurity and resilience objectives.** Sovereignty and cybersecurity should therefore reinforce one another through risk-based, evidence-driven requirements, with disproportionate annual revalidation for UAL 2-4 replaced by continuous monitoring and reassessment after material changes.

6. Procurement and EU-added value

The EU’s cloud and AI ecosystem can benefit from a shift towards procurement criteria that value innovation, sustainability and interoperability alongside price. CADA should promote interoperable, multi-cloud environments that prevent vendor lock-in and preserve public authorities’ ability to

choose the solutions that best meet their operational needs. The derogation mechanism under Article 30(4), which provides a necessary route for public sector bodies to procure cloud and AI services outside the UAL framework in situations of emergency or operational necessity, is therefore a positive step. More broadly, CADA should avoid procurement rules that unnecessarily restrict competition or reduce access to innovative services. Where compliance would impose disproportionate costs, a clear proportionality mechanism should apply across the framework, while excluding costs arising from vendor lock-in practices.

Conclusion

AmCham EU supports the EU's digital sovereignty objectives and the ambitions underpinning CADA. The Cloud and AI Development Act can make an important contribution to Europe's competitiveness, resilience and digital transformation – provided its sovereignty framework is based on demonstrable risk, operational resilience and effective safeguards rather than origin-based restrictions.

The co-legislators should ensure that the framework remains proportionate, technology-neutral and operationally feasible, while preserving competition, interoperability and cybersecurity. CADA should also remain focused on public sector procurement and avoid duplicating requirements already addressed through DORA, NIS2 and other sector-specific resilience frameworks. AmCham EU stands ready to engage constructively with the European Parliament and Council as the legislative process progresses.