Digital sovereignty that delivers



Five practical improvements to strengthen the Cloud and AI Development Act

The Cloud and AI Development Act (CADA) offers an opportunity to strengthen Europe's cloud and AI ecosystem and build trust in digital infrastructure. The question is how best to achieve these goals.

As currently envisaged, CADA introduces origin-based restrictions that are not necessarily linked to sovereignty. These measures could reduce competition, increase costs and slow cloud and AI adoption – ultimately working against CADA's underlying objectives. An alternative risk-based approach will strengthen Europe's digital competitiveness while preserving cybersecurity, interoperability and supplier choice. These five refinements would help CADA follow that risk-based approach:

Current approach	Unintended consequence	Fix
01. Avoid duplication of existing rules		
Article 31 and related sovereignty assessments can overlap with existing resilience and third-party risk requirements already established under DORA, NIS2 and sector-specific frameworks.	Additional sovereignty requirements create duplicative compliance obligations and legal uncertainty. Sectors like financial services already manage these risks through dedicated supervisory frameworks.	Keep CADA focused on public-sector procurement and avoid duplicating requirements that are already addressed by existing financial services and critical infrastructure legislation.
02. Establish different rules for different cloud services		
CADA applies the same cloud framework across infrastructure (IaaS), platforms (PaaS) and software applications (SaaS), despite their very different risk profiles.	One-size-fits-all requirements create disproportionate burdens. A payroll or accounting application does not create the same sovereignty risks as infrastructure hosting critical government workloads, for example.	Apply requirements according to the service model, workload criticality and data sensitivity. Reserve the strictest requirements for genuinely critical infrastructure-layer services.

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Current approach	Unintended consequence	Fix
03. Enable global threat visibility		
CADA treats telemetry and metadata as customer data and therefore subjects them to localisation requirements.	Telemetry helps identify attacks and share threat intelligence across global networks. Restricting its processing and analysis could weaken cybersecurity, incident response and service reliability.	Distinguish customer production data from operational data such as telemetry and metadata. Localisation requirements should focus on data that presents genuine sovereignty risks.
04. Limit regulation to genuine cloud services		
CADA's scope risks capturing services that are simply hosted on cloud infrastructure, rather than cloud services that rely on scalable and elastic pools of computing resources.	This could create legal uncertainty, divert audit resources away from higher-risk services and impose disproportionate burdens on lower-risk providers.	Limit the assurance framework to genuine cloud computing services as defined under NIS2 and focus requirements on services that present the systemic risks CADA is intended to address.
05. Focus on real services disruption risks		
Several sovereignty criteria and equivalence requirements are linked to potential third-country disruption scenarios and restrictions on service continuity.	Broad assumptions about disruption risk may exclude providers that have strong operational safeguards and resilience mechanisms in place, reducing choice without necessarily improving continuity or security.	Assess service disruption risks through demonstrable operational resilience, continuity planning and security safeguards rather than origin-based assumptions. Restrictions should be based on evidence of risk.