CISPE Response to CADA Public Consultation

CISPE welcomes the intent and guiding principles of the Cloud and AI Development Act (CADA). Mandating sovereign cloud solutions is the right way to reduce dependence and build Europe's strategic autonomy in the digital sector. That autonomy comes from choice and control, and CISPE stands ready to help deliver it: its Sovereign and Resilient Cloud Services Framework already gives cloud and AI vendors two equally robust ways to demonstrate that their services meet customers' expectation of control. As drafted, CADA hinders rather than supports Europe strategic autonomy in cloud and AI.

- It sets a technical bar that sovereign European providers cannot clear while hyperscalers-backed joint ventures can;
- It builds a register of trusted services but gives public buyers no reason to use them;
- It leaves loopholes through which foreign-controlled services can be resold as sovereign, and;
- It makes providers prove again what independent audits have already established.

Five critical fixes, described below, put this right without changing the Act's architecture or its level of assurance. Further improvements are also suggested below.

Five critical fixes are needed to ensure CADA delivers – and does not become the 'Continued American Dominance Act'

1. **Do not exclude European providers from Levels 2, 3 and 4** through source-code audits that make foreign software companies kingmakers over European sovereignty.
2. **Mandate 'Buy European or Explain'** to deliver on market-share ambitions.
3. **Close the Annex II loopholes** that let foreign companies, their joint ventures and critical subcontractors qualify as sovereign.
4. **Recognise existing certified frameworks and evidence** to minimise the burden on SMEs.
5. **Make trusted-country status objective, and make it count.** UK, Switzerland, Norway and Iceland included from day one

1. Remove the source code audit to ensure the CADA does not exclude European companies due to requirements only hyperscalers joint ventures can meet.

For Level 2 and 3, Annex II requires a source-code audit of security-relevant software components supplied by third-country manufacturers.[1] In a typical independent European stack these are the building blocks - virtualisation, operating systems, security, networking and AI accelerator software[2] - that most often come from third-country vendors such as Broadcom/VMware, Microsoft, Cisco and Nvidia. A European provider uses them under licence and cannot compel the vendor to open its code for audit. A non-European hyperscaler, however, controls auditors' access to its own code, and a joint venture given access by its parent (Delos Cloud, S3NS) can open that code to auditors itself. An independent European provider running the very same components cannot.

The requirement therefore measures who owns the code, not who controls the service, and rewards the third-country dependency CADA is meant to reduce. Its security value is also limited: a biannual audit is relevant only on the day it is performed, while software vendors collectively release hundreds of critical fixes every month.

[1] This goes beyond what NIS 2 or ISO 27001 require. "Security-relevant" is not defined in CADA. For the purposes of this response, we read it, by reference to the Cyber Resilience Act (Article 7, Recitals 43–45 and Annex III) and Regulation (EU) 2025/2392, as covering software categorised as important products with digital elements in Classes I and II.

[2] Including hypervisors and virtualisation software, host operating systems, firewalls, VPN, anti-virus and anti-malware software, identity and access management, TPM and key-management firmware, GPU and AI accelerator software.

Should there be insistence on this requirement CADA should place the audit obligation on the third-country manufacturer *or* accept a recognised independent evaluation of the component instead[3] and should recognise - as Scenario 1 "Loopholes and circumventions" below shows - that the relevant test is not access to source code but whether a third-country entity can disrupt the service, assessed in proportion to how much of the platform depends on it.

2. Mandate 'Buy European – or Explain' for cloud and AI services.

Nowhere does the current text call for 'Buy European or Explain'. Listing European services in the registry of 'accredited' services is not a mandate to buy them, and European 'value-add' is not a substitute for European control (bottling US wine in France does not make it French). CADA leaves purchasing behaviour untouched: a public buyer may choose any recognised service, even where an equivalent offering free of third-country jurisdiction competes against one that is subject to it, and the only preference for European value-add is an ancillary award criterion.

At a minimum, CADA should oblige a public authority to check whether a European service exists before awarding public money to a provider controlled from outside Europe, and to explain publicly when it does not choose one. This is a duty to look, not a duty to prefer; it is basic due diligence with taxpayers' money, not a barrier to trade. Without it, assessments risk becoming a rubber-stamp exercise that lets IT departments keep buying non-sovereign services out of convenience.

3. Close the loopholes in Annex II that exclude critical subcontractors from the audit

As drafted, critical subcontractors can escape the audit required for Assurance Levels 3 and 4, so no one assesses whether the service is subject to third-country control. Most importantly, because a subcontractor is only in scope if the CSP holds a direct contract with it, any foreign-controlled service can be resold as sovereign simply by interposing a European distributor as contract holder. The Annex below sets out the loopholes in detail.

4. Recognise existing frameworks and their evidence – SMEs shall not pay twice.

European frameworks such as EUCS, BSI C5, SecNumCloud, ENS Alto, Gaia-X Level 3 and the CISPE Sovereignty and Resilience Frameworks already have cloud services independently audited against control, jurisdiction, personnel, data-location, exit and continuity requirements that match or exceed Annex II. CADA would make a certified provider pay twice for the same controls – a burden that falls hardest on SMEs. A single rule of evidence should apply: a certificate under a recognised scheme counts for the criteria it demonstrates, proven once. Recognition should also attach to the service, not the company, and detailed audit results should be public.

Annex III lets auditors consider any evidence they choose, but does not require recognising existing certifications, specifications and standards as evidence for the Annex II criteria. That recognition, not auditor discretion, is what would cut SMEs' compliance costs under the Union assurance levels.

5. Make trusted-country status objective, and make it count.

The United Kingdom, Switzerland, Norway and Iceland should be trusted by default from the day CADA applies, rebuttable only by a reasoned Commission decision identifying a specific, evidenced problem. Each already meets the criteria Article 18 should turn on – participation in EU-anchored infrastructure such as EuroHPC and a valid adequacy decision – and a two-to-three-year designation process withholds allied capacity from European buyers for no sovereignty gain. Designation should rest on objective, publicly verifiable criteria rather than administrative discretion, with providers from qualifying countries presumed eligible for Level 3. The status must then carry through: Annexes II and III should treat ownership, investment, board composition, operational control and personnel in trusted countries and the EEA as equivalent to their EU-27 counterparts.

[3] For example, an EUCC certificate, a CRA conformity assessment, or an evaluation by an EU-accredited laboratory.

Further improvements that can strengthen the positive impact of an updated CADA.

1. Tie European taxpayer funds to Sovereign Cloud Credits. EU funding for research and digital development should be spent with sovereign European companies; a system of sovereign cloud credits would ensure European customers benefit from European cloud and AI services.

2. Extend the timeline for switching to mandated sovereign solutions. One year is inadequate for most public (or private) sector migrations; unrealistic time pressure will push customers towards joint ventures set up by their existing hyperscale providers. The Broadcom/VMware experience, where organisations struggle to switch even in three years, proves the point.

3. Confirm that open-source software commercialised as an enterprise-grade product remains 'open source' under CADA. Software released under a recognised open-source licence and also distributed with enterprise support – enterprise Linux being the clearest example – should continue to qualify. A narrower reading would confine the concept to unsupported community distributions and penalise precisely the European vendors that invest in hardening, certifying and supporting open source for professional and public-sector use.

4. Treat European proprietary software like open source. Proprietary software developed and maintained in the Union by companies free of third-country control presents none of the sovereignty exposure CADA is designed to address. Annex II already accepts this in one place: its source-code audit applies only to components from third-country manufacturers. That logic should apply consistently across all Annex II and III criteria – control, personnel and audit – so that such software is sovereign by default, without a source-code audit, and European vendors are not disadvantaged against third-country suppliers when their products are embedded in publicly procured cloud and AI services.

5. Do not call Levels 1,and 2 'sovereign'. Level 3 is robust, possibly 'resilient' based on CISPE requirements, but not 'sovereign' since it allows for services subject to the control of third country to be eligible. Labelling those services 'sovereign' in any way will confuse buyers and encourage further sovereignty washing.

6. Rebalance the enforcement burden and allow designations to be challenged. Any Member State may designate a vendor as 'sovereign', but only the one hosting its European headquarters can enforce the decision, concentrating the burden on a few countries. Other Member States and individual vendors should be able to challenge designations that distort competition.

7. Reinforce competition and interoperability and prevent anti-competitive bundling of AI and cloud services. CADA should support federated European cloud initiatives and ensure that the AI capacity it funds or recognises cannot be used to lock customers into a single provider's cloud through bundling or restrictive licensing – the practices that entrenched the dominance the Act seeks to reverse.

Annex: Loopholes and circumventions of CADA Sovereignty Assurance Levels

The structural challenge of Annex II, Sections 3.2 and 4.2

Annex II, Sections 3.2 and 4.2 define an audited subcontractor as a third party that (i) has a direct contract with the Cloud Computing Service Provider, (ii) contributes to delivery of the service, AND (iii) may require access to classified or sensitive information. All three conditions are cumulative; if any one fails, the entity falls outside the Annex II audit and the Annex III guidance, and no one assesses whether it places the service under third-country control. The two scenarios below show how entities posing a material sovereignty risk escape the audit perimeter on this basis.

Overview — The Structural Pattern Across Both Scenarios

Both scenarios (Microsoft/Delos and AI aggregation) turn on the first criterion: the US vendor has no direct contract with the Cloud Computing Service Provider, so it is never assessed, even though it controls the software supply chain and can render the service inoperable through update denial or licence withdrawal under US legal compulsion.

The fix is to extend the audit perimeter to any entity – software vendor, corporate parent, licensor or infrastructure intermediary – able to disrupt the service under third-country compulsion, regardless of data access, with the assessment proportionate to the dependency. Whole-platform dependency (Scenario 1) must disqualify a service from Levels 3 and 4; a replaceable component with a credible exit plan should be assessed and mitigated, not used to exclude independent European providers (see critical fix 1).

Left unaddressed, these loopholes reduce the Assurance Levels to sovereignty washing and place foreign technology on an equal – or higher – footing than competing European offerings.

Criteria status across both scenarios

Scenario / Third Party	3.2 Criterion 1 (Direct contract)	3.2 Criterion 2 (Service delivery)	3.2 Criterion 3 (Data access)	Audit outcome
S1 – Microsoft / Delos (DE)	✗	✓	✗	**Excluded**
S2 – Aggregation: AI	✗	✓	✓	**Excluded**

Scenario 1 — Third-Country Partnership: Delos / Microsoft Azure (Germany)

Delos Cloud is a German public-sector cloud platform operated by an SAP subsidiary: contractually independent from Microsoft, physically separated from global Azure, run by cleared German personnel, with updates vetted by the BSI. It holds the right to use Microsoft's code should sanctions restrict Microsoft's services in Europe and presents itself as meeting German federal sovereignty requirements.

Yet the entire stack – hypervisor, IaaS, PaaS and Microsoft 365 – is Azure software developed and updated by Microsoft, a US entity under US jurisdiction. Microsoft should arguably be a subcontractor in the Annex II sense, but Arvato Systems (the audited provider selling to public-sector customers) may have no direct contract with Microsoft, and Delos states that Microsoft does not access sensitive data – so neither the first nor the third criterion is met. The exposure is nonetheless structural: every patch originates in the United States, and a US order to stop supplying them would progressively degrade the platform until it became inoperable or insecure, source-code access notwithstanding. Source-code access is therefore no guarantee of sovereignty (see critical fix 1), and this is precisely the disruption risk Section 3.1 of Annex II should prevent.

Third party assessed: Microsoft (US) — Azure software licensor to SAP/Delos Cloud

Section 3.2 Criterion	Status	Explanation
Direct contractual relationship with the Cloud Computing Service Provider (Art. 3.2 §1)	✗ **Not met**	Microsoft has no direct contractual relationship with the Cloud Computing Service Provider (Arvato) offering services to public sector end customers. The relevant contractual relationship is arguably between Microsoft and SAP/Delos Cloud GmbH — not Arvato Systems, an intermediate entity. This is the first criterion that is arguably not met.
Contributes to the provisioning and delivery of the cloud service (Art. 3.2 §2)	✓ **Met**	The entire Delos Cloud stack — hypervisor, IaaS, PaaS, Microsoft 365 — runs on Azure software. Microsoft's contribution to provisioning and delivery of the cloud service is total and irreplaceable.
May require access to classified or sensitive information processed by the service (Art. 3.2 §3)	✗ **Not met**	Microsoft personnel have no access to classified or sensitive customer data held on the Delos Cloud platform. The BSI audits updates before deployment and German personnel operate the environment. Failure on both the first and third criteria places Microsoft entirely outside the Section 3.2 subcontractor definition.

Sovereignty disruption risk: Microsoft controls the entire Delos software supply chain; a US order to cease updates would degrade the platform to inoperability without Microsoft accessing any customer data.

Result: Microsoft is NOT a subcontractor under Section 3.2 (first and third criteria not met). A service built on Delos/Azure can be certified at Level 3 or 4 while its existential dependency on a US vendor able to disable the platform appears nowhere in the Annex II audit.

Scenario 2 — Aggregation and Routing: SaaS Provider Using AI

Many SaaS products now embed generative AI. In this scenario the SaaS provider has no GPU compute of its own and relies on an AI aggregation and routing subcontractor – European examples include opper.ai and EdenAI – which offers inference across hundreds of models hosted on a variety of clouds, including AWS. We use models running on AWS Bedrock in European regions, but the analysis is the same for any third-country cloud, and similar aggregation and routing services exist for other types of cloud service. The Cloud Computing Service Provider contracts only with the aggregator, not with the AI model and GPU compute provider (here AWS) – even though a significant component of the service is delivered by that provider.

Third party assessed: Amazon Web Services

Section 3.2 Criterion	Status	Explanation
Direct contractual relationship with the Cloud Computing Service Provider (Art. 3.2 §1)	✗ **Not met**	Amazon Web Services has no direct contractual relationship with the Cloud Computing Service Provider (SaaS provider), but sells its GPU compute and model inference to the AI Aggregator / Router.
Contributes to the provisioning and delivery of the cloud service (Art. 3.2 §2)	✓ **Met**	Amazon Web Services' Bedrock service runs the GPU inference, contributing a part of the cloud service.
May require access to classified or sensitive information processed by the service (Art. 3.2 §3)	✓ **Met**	Amazon Web Services may require access to data processed as part of the inference. This could include sensitive information.

Sovereignty disruption risk: AWS controls the inference layer of the service. A US order could compel it to cease service (via export controls, sanctions or executive action) or to hand over customer data processed in Bedrock.

Result: AWS is NOT a subcontractor under Section 3.2 because the first criterion – a direct contract with the Cloud Computing Service Provider – is not met, even though it both delivers part of the service and may access sensitive data. A SaaS service can thus be recognised as sovereign while its AI inference runs on, and its data passes through, a US hyperscaler that never appears in the audit.

Annex 2: Security-relevant software: no cloud provider has the source code

The issue. The Cloud and AI Development Act (CADA) makes eligibility for sovereignty levels 2 and 3 conditional on the provider ensuring source code audit, by ensuring the independent auditor is granted the right to access and audit the source code of the "security-relevant" components of its service — a term the Act does not define. Read by reference to the Cyber Resilience Act (Art. 7, Recitals 43–45, Annex III, and Regulation (EU) 2025/2392), it covers the "important" products in Classes I and II: hypervisors, host operating systems, firewalls, VPN, anti-malware, identity and access management, TPM and key-management firmware, GPU and AI accelerator software, and core networking software. These are unavoidable components every cloud service is built on.

The fact. In every one of those layers, the products that European providers actually run are supplied as binaries, firmware or managed services under licences that grant no access to source code. This is true of the US market leaders and equally true of the European vendors (Thales, Infineon, Stormshield, Bitdefender, ESET, Nokia): proprietary is the industry norm, not an American peculiarity. Even a provider running a fully open-source software stack sits on closed firmware in the CPU, BIOS, management controller, network card, GPU and switch silicon beneath it. Vendor "source review" programmes (Microsoft GSP, Huawei) are NDA-bound, and reserved for governments. Even here, a bi-annual review would fail to provide protection against the thousands of vulnerabilities discovered and patched monthly. As such, the requirement adds little in the form of security.

The consequence. A source-code audit condition for levels 2 and 3 cannot be met by anyone in Europe today, except perhaps joint ventures with foreign hyperscalers. Applied as drafted, it would disqualify most European providers from the very market the Act is meant to open to them, and elevating hyperscalers, who control many such components outright, to a role of "kingmaker" in granting access. The table shows, per layer, example software components European providers rely on and the answer to the only question that matters: can the provider give the auditor source code access?

Security layer (CRA class)	Most widely used products in European cloud estates — vendor (HQ)	Provider has source code?
Hypervisor (II)	VMware vSphere / ESXi — Broadcom (US); Hyper-V — Microsoft (US); Nutanix AHV — Nutanix (US)	No
Host OS (I)	Windows Server — Microsoft (US); RHEL — Red Hat / IBM (US); SUSE — SUSE (EU) – open, but closed firmware and bios beneath	No
Firewall / IPS (II)	PAN-OS — Palo Alto Networks (US); FortiOS — Fortinet (US); Check Point — Check Point (IL)	No
VPN / remote access (I)	AnyConnect — Cisco (US); GlobalProtect — Palo Alto Networks (US); FortiClient — Fortinet (US)	No
Anti-malware / EDR (I)	Falcon — CrowdStrike (US); Defender — Microsoft (US); SentinelOne — SentinelOne (US)	No
Identity & access (I)	Entra ID / Active Directory — Microsoft (US); Okta — Okta (US); CyberArk — CyberArk (IL)	No
Keys, TPM, HSM (II / Annex IV)	Intel CSME / AMD PSP firmware — Intel / AMD (US); Luna HSM — Thales (EU) – closed; nShield — Entrust (US)	No
GPU / AI (I)	CUDA + GSP firmware — NVIDIA (US); ROCm firmware — AMD (US); Neuron — AWS (US)	No
Networking (I)	IOS / NX-OS — Cisco (US); Junos — Juniper / HPE (US); Switch ASIC SDK — Broadcom (US)	No
SIEM (I)	Splunk — Cisco (US); Sentinel — Microsoft (US); Google SecOps — Google (US)	No

What CISPE asks

- Remove the source-code audit requirement from the eligibility criteria for levels 2 and 3.
- Alternatively, replace it with a reference to obligations around assessment of software, patches, and updates from the EUCS or similar high level cyber-security standards.
- Apply the same test to every provider, so that ownership of proprietary components does not become a privilege reserved for the largest non-EU vendors.

-End of Submission-