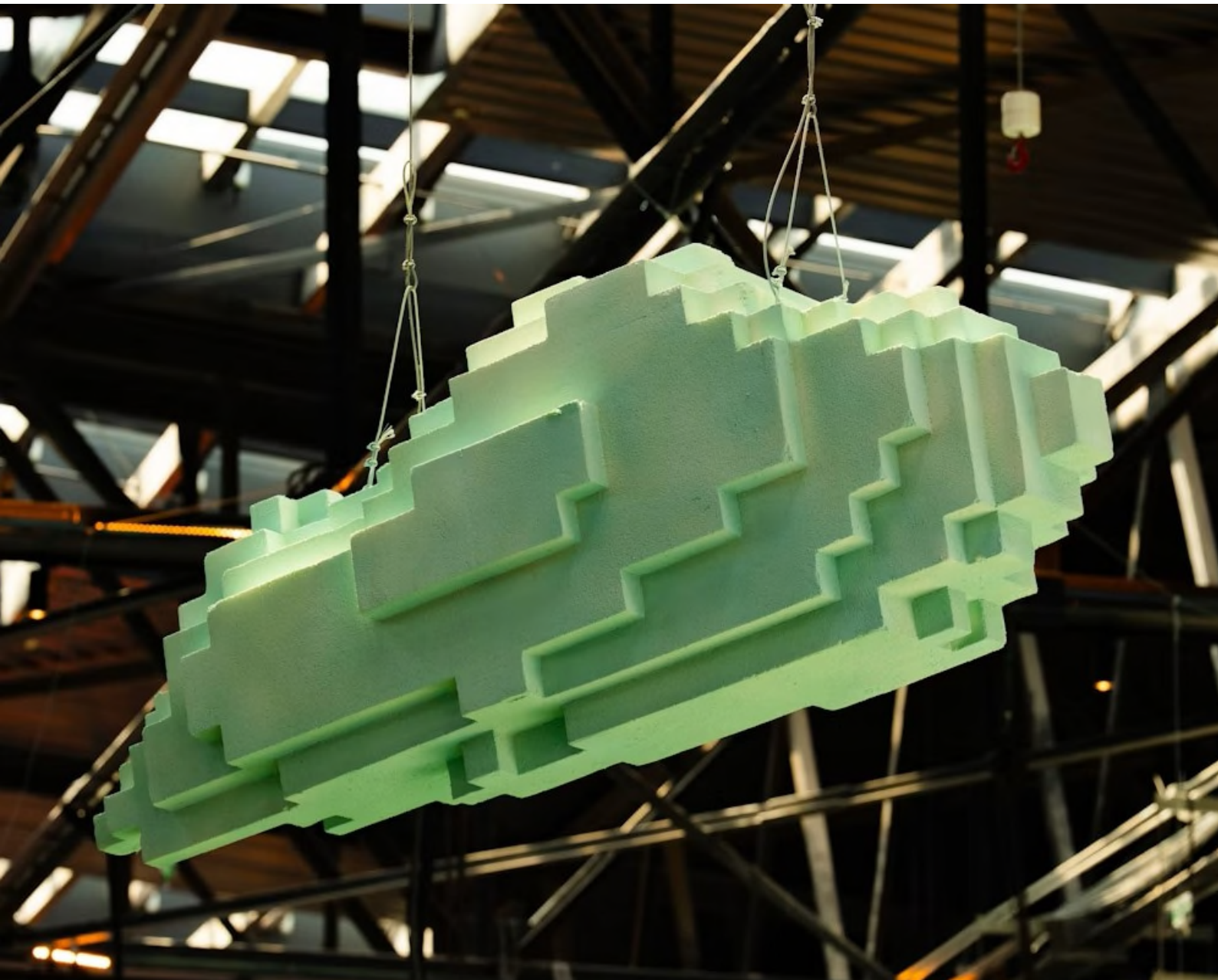
TÜV VERBAND

November 2026

Position on the Tech Sovereignty Package's CADA

Cloud & AI Development Act



Introduction

Europe's technological sovereignty depends not only on its ability to develop and control critical technologies, data systems and infrastructure, but also on its capacity to assess and manage dependencies on non-EU providers. This dual objective is reflected in the proposed Cloud and AI Development Act (CADA, COM(2026) 502) published in June 2026 as part of the EU's Tech Sovereignty Package and wider AI Continent Action Plan, which aims to strengthen Europe's technological sovereignty and competitiveness in the cloud and AI ecosystem. It seeks to foster innovation and investment, expand Europe's data centre and computing capacity, and facilitate the deployment of sustainable cloud and AI infrastructure. At the same time, CADA would introduce a common EU-wide sovereignty framework with four Union assurance levels, particularly relevant for public authorities procuring cloud services based on their risk assessments. Together, these measures aim to reduce critical dependencies and accelerate the adoption of cloud and AI in strategic sectors.

The TÜV Association welcomes the European Commission's proposal as it rightly recognises that Europe's economic and geopolitical capacity to act depends not only on the rules laid down for trustworthy technology such as the AI Act, but also on secure access to cloud, computing and AI infrastructure. Given the Commission's assessment that the Union still relies on non-EU providers for over 80 percent of digital products, services or infrastructure, reducing critical dependencies and ensuring secure access to key digital infrastructure is essential to strengthening Europe's resilience. At the same time, the EU's large and economically attractive single market of around 450 million citizens gives global cloud service providers a commercial incentive to maintain access to the European market and demonstrate compliance with EU sovereignty requirements. Against this backdrop, it is essential that claims of cloud sovereignty are independently verified and supported by reliable evidence. Sovereignty audits can play a key role in this regard by assessing whether cloud services meet applicable assurance-level criteria for control and resilience under adverse legal, operational and geopolitical conditions.

This position paper focuses on the cloud sovereignty framework and its implementation through independent audits and public procurement. A harmonised approach as proposed by the CADA framework can help prevent "sovereignty washing" (false or misleading claims about independence from foreign control) by establishing clear and consistently applied criteria for assessing cloud sovereignty across the EU. For assurance levels two to four, CADA should ensure an open, competence-based market for sovereignty audits and explicitly allow qualified independent testing, inspection and certification (TIC) organisations to participate alongside other qualified auditors. Given the multidisciplinary technical expertise required for assessments at these levels, including in cloud architecture, software and supply-chain dependencies, data flows and corporate control structures, auditor eligibility should be based on technical competence, relevant assessment experience and importantly, their demonstrated independence. This would support the consistent application of sovereignty requirements, help identify critical dependencies and vulnerabilities, prevent misleading sovereignty claims and ultimately

strengthen the credibility of the EU's cloud sovereignty framework.

Key recommendations

CADA should turn sovereignty into a technically verifiable, risk-based assurance framework, assessed by competent independent auditors, interoperable with the EU's existing digital rulebook.

› **Ensure an open and competent market for independent audits**
Accurate and reliable classification is a fundamental prerequisite for CADA's effectiveness. Eligibility for audits at levels 2 to 4 should depend on demonstrated independence, technical competence and audit experience. Furthermore, robust third-party verification can help prevent "sovereignty washing" by ensuring that sovereignty claims are based on transparent, technically verifiable criteria rather than self-declaration or marketing claims.

› **Define clear and risk-based sovereignty requirements**
Sovereignty requirements should be sufficiently precise to enable meaningful and comparable assessments across providers and use cases. CADA should make sovereignty claims verifiable by clearly defining the scope of recognised services, assessing material dependencies and linking assurance requirements to the risks of relevant cases at hand. The criteria should focus on effective control and operational resilience rather than formal characteristics alone, while providing buyers with transparent and reliable information.

› **Create a consistent European assurance process**
Harmonize audit methodologies and evidence requirements across the EU, protect sensitive information and enable proportionate reuse of existing assessments, while maintaining robust independent verification and effective public oversight.

› **Require testable exit and recovery capabilities**
Critical cloud contracts should include testable requirements for portability, transition support, recovery and continuity. Exit and recovery plans should be tested in practice and, where appropriate, independently assessed to provide contracting authorities with verifiable evidence.

› **Connect CADA with existing assurance frameworks**
CADA should stay focused on cloud sovereignty while allowing targeted reuse of relevant existing evidence. Overlapping requirements should be mapped, but existing certificates and assurance reports should not imply automatic equivalence or replace sovereignty-specific verification.

Recommendations in detail

› **Ensure an open and competent market for independent audits**

CADA can only deliver credible sovereignty assurance if compliance is not merely declared but independently verified against clear and technically robust criteria. Especially for assurance levels 2 to 4, this requires auditors that can assess complex technical, organisational and supply-chain dependencies and translate them into a reliable assurance opinion.

CADA should therefore ensure an open, competence-based market for sovereignty audits and explicitly allow qualified independent TIC organisations to participate alongside other qualified auditors. Their eligibility should be based on demonstrated independence, technical expertise and relevant assessment experience. By providing independent and technically robust assessments, TIC organisations can help ensure consistent application of CADA's sovereignty requirements and strengthen confidence in the framework.

This is consistent with Section 3 on "Independent third-party audits", and in particular Article 20, "Independent audit", which sets the core requirements for such audits. Article 2(17) defines auditing organisations broadly, while Article 20(4a-c) already requires independence, technical competence and professional ethics. Eligibility should therefore build on these capabilities and recognise all organisations that can demonstrate the necessary competence. This would strengthen assessment quality, broaden audit capacity, reduce concentration in the assessment market and support the credible and consistent implementation of CADA's sovereignty framework.

Sovereignty audits pose a complex assessment as they may require technical scrutiny of cloud architecture, data flows, software dependencies and operational separation, privileged access, supported by legal and corporate-control analysis. Such assessments therefore require auditing organisations with proven, multidisciplinary expertise and substantial experience in complex technical assurance. Relevant existing accreditations and assessment experience of auditors should help demonstrate competence; however, a clear evaluation of any CADA-specific gaps must be conducted. Given their long-standing expertise in independent technical assessment, TIC organisations should be consulted as stakeholders where useful and could contribute to developing relevant methodologies where appropriate.

The prohibition of outcome-contingent fees and safeguards against conflicting non-audit services in Article 20(4a) should be retained. A proportionate and workable independence regime is essential to maintaining sufficient audit capacity and thereby supporting the reliable implementation of CADA's sovereignty framework and Europe's digital resilience.

› **Define clear and risk-based sovereignty requirements**

For CADA to provide meaningful and credible assurance, sovereignty requirements must be sufficiently precise to reflect the actual risks to control, continuity and resilience of cloud and AI services. They should therefore distinguish between different sources of dependency and focus on effective control rather

than formal characteristics alone.

Article 16(1), describing the scope of the assurance levels, and Annex II establish a four-level assurance framework intended to reflect different degrees of sovereignty and risk.

CADA's criteria for each assurance level should be clearly linked to the risks of the specific use case and distinguish between legal control, operational autonomy and supply-chain dependencies. In particular, criteria relating to location, citizenship and ownership should be tied to the specific risks they are intended to address and complemented by an assessment of effective control. Formal origin alone is not sufficient to demonstrate operational resilience.

For recognition to be meaningful, customers and public buyers need to understand exactly which cloud or AI service has been assessed and under what conditions. Article 22(1-4) governs how recognised services are listed and presented in the public repository. CADA should require the scope of recognition to be clearly defined, including the relevant service version or configuration, deployment model, regions, material dependencies and inherited controls. Information published under Article 22 should reflect this scope accurately and should not suggest that recognition of one service extends to a provider's entire portfolio. A clear, customer-readable assurance summary could further improve transparency by setting out the audited service, assurance level, period covered, latest review and current recognition status. This would give buyers more reliable information, strengthen supply-chain transparency and help prevent sovereignty washing.

Additionally, CADA should ensure that material dependencies are assessed wherever they can affect the sovereignty and resilience of a cloud or AI service, even if the underlying component falls outside the formal scope of the framework. In this context, the hardware exclusion in Annex II could be aligned with the hardware asset evidence under Annex III (2, "Audit criterion B"), and controls over firmware and BIOS modifications under Annex III (9, "Audit criterion I").

› **Create a consistent European assurance process**

A Union assurance level should provide a comparable degree of assurance across the EU, irrespective of the Member State in which a provider is established or the auditing organisation conducting the assessment. Without sufficiently harmonised audit methodologies and evidentiary expectations, the same Union assurance level could in practice be based on different levels of scrutiny, undermining comparability and trust in the framework across the Single Market.

The Commission should therefore use the delegated acts provided for in Articles 20(9) and 21(1) to establish a consistent European approach to assurance. Under Article 20(9), common rules on audit procedures, auditing methodologies, the technical competences of auditing organisations and audit-report templates should ensure that assessments are performed consistently across the Union. This should include common approaches to sampling, assessment and treatment of audit findings. Article 21 should complement these rules by operationalising requirements that audit evidence be relevant, sufficient and reliable and, where necessary, by further specifying in Annex III the evidence needed to

assess Annex II criteria.

Evidence requirements should remain proportionate and should not result in unnecessary transfers or retention of sensitive information. Passport copies, source code or sensitive corporate and security records, for example, should not have to be transferred or retained by default where secure inspection, controlled access or other less intrusive means can provide sufficient and reliable audit evidence. At the same time, auditors must have access to all information necessary to form a substantiated audit opinion and must retain the professional judgment and skepticism required by Article 21(2b) when assessing the reliability of evidence. Confidential annexes, purpose limitation and appropriate access controls should protect personal data, trade secrets and security-sensitive information without compromising the effectiveness of the audit.

Article 17(4-5) could better distinguish the role of the independent auditor and of the evaluating authority. As drafted, the audit report, the positive opinion and full body of evidence provided to the auditor are submitted to the evaluating authority and then again included in the notification to other Member States. This creates a risk that evidence already examined by a qualified independent auditor is routinely re-examined by public authorities. Such duplication would weaken the efficiency gains of the independent audit model, increase administrative burden and expose sensitive corporate, security and personal data to unnecessary circulation. It could also lead to different authorities reassessing the same evidence according to different expectations, reducing consistency across the Union.

CADA should therefore establish a clear principle of reliance on qualified independent audits. As a rule, the evaluating authority and other Member States should receive the substantiated audit report and positive opinion, while underlying evidence should remain available through controlled access where specific concerns, inconsistencies or supervisory needs justify further examination. Authorities should retain full recognition, investigation and oversight powers, but additional technical review should be targeted and risk-based rather than automatic. Common review criteria should further ensure that recognition decisions are consistent and that the same evidence is not repeatedly reassessed across Member States.

Moreover, audit evidence should be reusable where it is current, reliable and matches the relevant scope, particularly for shared infrastructure, common cloud components and subcontractors. The auditing organisation should verify its applicability, identify any gaps and remain responsible for the overall audit opinion. The annual review under Article 20(8) should confirm continued compliance and assess material changes. Changes affecting control, jurisdiction, architecture, privileged access or critical dependencies should be notified and assessed under Article 23(1-3), with the audit report, opinion or recognition amended or revoked where necessary, rather than waiting for the next annual review.

› **Require testable exit and recovery capabilities**

Procurement requirements for critical cloud services should go beyond contractual commitments and make resilience and exit capability independently verifiable. Contracts should therefore include clear and testable requirements for portability, transition support, recovery, material-change notification and

access to relevant assurance evidence.

Exit and recovery plans should be tested in practice and, where appropriate, independently assessed by qualified third parties. This would provide contracting authorities with reliable evidence that switching, recovery and continuity arrangements are effective, while leaving the final risk decision with the public authority.

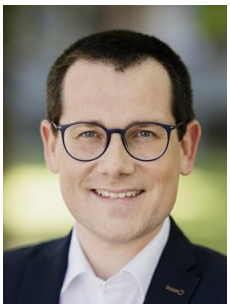
› **Connect CADA with existing assurance frameworks**

A CADA assurance level should be clearly understood as an assessment of cloud sovereignty requirements. It must not, for instance, be presented as evidence that an AI system complies with the AI Act, or that a cloud service is certified under a cybersecurity scheme, even where individual requirements overlap. Clear boundaries are needed to avoid misleading compliance claims, double counting and legal uncertainty. At the same time, CADA should enable targeted reuse of existing assurance evidence. The Commission, together with ENISA and relevant standardisation bodies, should map overlapping requirements across CADA, the Cybersecurity Act and applicable cloud cybersecurity schemes, NIS2, Cyber Resilience Act, Data Act, AI Act and relevant sectoral frameworks. Existing certificates and assurance reports, including ISO 27001, C5 or SOC 2, should support CADA only where their scope, period, findings and control effectiveness are demonstrably relevant (and not be treated as automatically equivalent or a substitute for sovereignty-specific verification.

Authors and contact persons



Mathea Essinger
Head of Brussels Office
E-Mail: mathea.essinger@tuev-verband.de
Tel.: +49 30 760095 485



Dr. Patrick Gilroy
Head of AI & Education
E-Mail: patrick.gilroy@tuev-verband.de
Tel.: +49 30 760095 360

As TÜV-Verband e.V. (TÜV Association), we represent the political interests of the TÜV testing organizations and promote professional exchange among our members. We are committed to technical and digital safety as well as the sustainability of products, systems, and services. This is based on universally applicable standards, independent testing, and qualified continuing education. Our goal is to maintain a high level of technical safety, build trust in the digital world, and preserve our livelihoods. To this end, we engage in regular stakeholder dialogue with politicians, authorities, the media, companies, and consumers.

Publisher
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
Fax: +49 30 760095-401
E-Mail: berlin@tuev-verband.de
www.tuev-verband.de