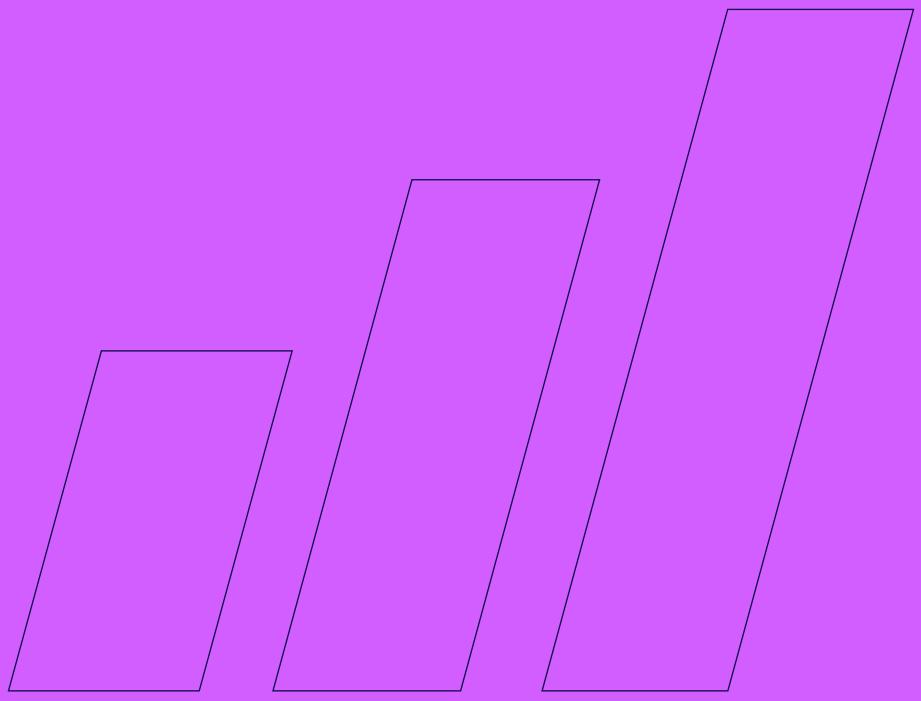
FOTI



Strengthening the EU's Cloud & AI Development Act

Step 2: Set a Strong Standard

How to define and recognise sovereign services

A report series by FOTI
November 2026

FOTI

About FOTI

FOTI is a European think tank dedicated to building a prosperous and fair future that harnesses the power of technology.

We help democracies tackle some of the biggest technology challenges of our time. From market concentration and digital sovereignty to platform accountability and industrial policy, we develop practical solutions that strengthen innovation, support challengers and deliver better outcomes for people and societies.

About this series

Strengthening the EU's Cloud & AI Development Act is a report series by FOTI.

Step 2: Set a Strong Standard: How to define and recognise sovereign services
Strengthening the EU's Cloud & AI Development Act
November 2026

Table of contents

01 Executive summary 04

02 Context:
You can't guarantee sovereignty without verifiable standards 05

- How sovereignty is defined and claimed today 06
- How sovereignty is verified today 06
- What CADA does to address this 07

03 CADA's weakness:
As is, sovereignty will remain unverified 10

04 Our proposed fixes 13

- A. Ensure independent authorities 14
- B. Transparency requirements for the cloud sovereignty framework 17
- C. Improve the definitions in Annex II and Article 18 21

Sources and resources 26

01 / Executive summary

Today, a sovereign cloud service in Europe is whatever its provider says it is. Aside from marketing claims, no mechanism sets standards for operational autonomy or protecting data against foreign interference. But without common regulatory criteria, the definition of sovereignty will de facto be dictated by today's dominant hyperscalers.

The solutions that should have verified those claims have failed to deliver. The European cybersecurity certification scheme for cloud services (EUCS) has been stalled since 2019 under intense political pressure, while divergent national qualifications like France's SecNumCloud fragment the Single Market. Public buyers and enterprise customers are presented with "sovereign" solutions that, despite the label, leave foreign dependencies intact.

CADA gives Europe, for the first time, a common and auditable definition of sovereign cloud services, with four assurance levels, independent audits and Union-wide recognition.

But, as drafted, the framework leaves serious vulnerabilities and loopholes that threaten to deepen our dependencies on foreign providers dressed up as "sovereign services". Level 1 mandates only an unverified self-declaration that says virtually nothing about third-country control. Recognition is entrusted to national authorities that are not required to be independent. Additionally, the criteria are reviewed behind closed doors, and Annex II contains ambiguities that could allow foreign dependencies right back in under a "sovereign" label.

We recommend establishing independent national supervisory authorities (A.1); introducing transparency requirements for hardware (B.1); mandating software supply chain disclosures at Level 1 (B.2); opening the review and amendment process to democratic and public consultation (B.3); closing drafting loopholes in Annex II (C.1); reversing the burden of proof for source code audits (C.2); and clarifying adequacy decisions for associated third countries (C.3).

02 / Context:

You can't guarantee sovereignty without verifiable standards

Reducing a dependency requires agreeing on what freedom from it looks like. This section sets out how sovereignty is defined and claimed on the European cloud market today, how those claims are verified, and what the proposal does about it.

How sovereignty is defined and claimed today

Page 6

How sovereignty is verified today

Page 6

What CADA does to address this

Page 7

How sovereignty is defined and claimed today

There is no common definition, and claims are often overstated. The Commission's impact assessment states that current sovereignty claims "are made without demonstrating the safeguarding of operational autonomy and the protection of data against foreign interference or access", creating "an information asymmetry – as users do not have a reliable means of verifying whether a service is truly sovereign or not". The Commission concludes that without harmonised criteria "sovereignty claims would remain self-declared and the notion of sovereignty risks remaining a marketing tool with little or no effect in trust building". The assessment highlights the emergence of "sovereignty washing" alongside complaints from European SMEs that "foreign-controlled firms market services as 'European' despite extra-territorial dependencies".

The sovereign label is mostly applied by the providers Europe depends on. The impact assessment finds that non-European service providers, including US-based CSPs, are at the forefront of offering sovereign-branded solutions for the EU market – including the AWS European Sovereign Cloud, Oracle's EU Sovereign Cloud, and joint ventures such as Bleu (Capgemini and Orange offering Microsoft services) and Clarence (Proximus and LuxConnect on Google technology), priced at premiums estimated between 10% and 30% above public cloud rates. The proposal's recitals concede that such tailored versions "do not address the core sovereignty issues allowing for the extraterritorial reach of third-country laws and the possible degradation or disruption of the service".

Definitions of sovereignty vary from one jurisdiction to the next. Several Member States have developed national approaches to identifying sovereign services that the proposal acknowledges "risk fragmenting the Union internal market". The most developed is the French SecNumCloud qualification, which pairs strict technical cybersecurity criteria with non-technical sovereignty requirements; while France mandates qualified services for sensitive public data, overall market adoption remains low. In parallel, the Commission created an internal Cloud Sovereignty Framework of 48 criteria scored into Sovereignty Effectiveness Assurance Levels (SEAL) for its own procurement, which it encourages public and private buyers to consult.

How sovereignty is verified today

The Union instrument designed to certify cloud services has not been delivered. ENISA has been working on the European cybersecurity certification scheme for cloud services (EUCS) under the Cybersecurity Act since 2019, but it has not been adopted. The Commission's evaluation of the certification framework, published in January 2026, records that discussions on the EUCS "stalled over non-technical debates like data localisation requirements" and that the scheme "was impacted significantly by debates around data sovereignty requirements, drawing political pressures from third countries and industry outside the EU". CADA nonetheless builds upon this incomplete foundation: Levels 2 and 3 require a certificate at level "substantial" and Level 4 at level "high" under a European scheme that does not yet exist, leaving national

schemes to fill the vacuum in the interim.

What CADA does to address this

The proposal establishes a Union cloud computing sovereignty framework built on four assurance levels, supported by rules on updating criteria, recognising services, and managing enforcement.

Article 16 establishes the Union cloud computing sovereignty framework, comprising four Union assurance levels, with criteria set out in Annex II and audit evidence in Annex III. Providers must meet them in order to provide their services to Union entities and public sector bodies. The Commission may amend both Annexes by delegated act and must review them at least every 18 months to keep them up to date with legal and technical developments.

Annex II defines the four Union assurance levels. Software, as defined in the Cyber Resilience Act, is within scope; hardware is expressly outside it. All four levels rest on a common core – the provider is established in the Union, its infrastructure and assets are located there, customer data remain in the Union, the service meets a cybersecurity requirement, and technical support and exposure to third-country influence are regulated – and differ in how strictly each element is met:

Level 1 is the baseline: territorial anchoring of the provider, its assets and the data, state-of-the-art cybersecurity, and transparency over subcontractors. The public sector body may derogate from the location rules for infrastructure, assets and data, and providers under third-country control are admitted, subject only to a guarantee that the third country does not require early reporting of software vulnerabilities to its authorities.

Level 2 adds operational immunity and supply chain controls. The provider must demonstrate that third-country control cannot be used to restrict the service, access customer data, disrupt the service or impose foreign sanctions; that supply chain measures are in place (e.g. software bill of materials, controls blocking remote features, source code audits; migration plan); that technical support is performed exclusively within the Union; that service data are not used to train third-country AI systems; and that the service holds a cybersecurity certificate at level “substantial” under the future European scheme for cloud services.

Level 3 excludes third-country control unless the Commission has recognised the third country concerned as an "associated third country"; requires personnel to be Union citizens and support staff to be Union residents; and limits the subcontractors covered to those that may require access to classified or sensitive information.

Level 4 closes the remaining gap: third-country control is excluded absolutely, the cybersecurity certificate is required at level "high", and the provider must demonstrate that no third country or third-country entity holds effective control over the design, development, maintenance and evolution of the software components it relies on.

The impact assessment estimates which providers could reach each proposed level today: at Level 1, "US hyperscalers generally all have offerings that would allow them to qualify"; at Level 2, the "sovereign joint ventures" between US hyperscalers and European companies, with a hyperscaler's software stack and a security layer controlled by the EU partner; at Level 3, European providers, provided they obtain the future EUCS certificate and demonstrate "a 'very high' control over their software supply chain"; and at Level 4, "some emerging EU offerings", at least for some types of service. The Commission expects the two highest levels to be needed for about 10% of public sector use cases. We believe such a small percentage of the public market for Level 3 and 4 cannot provide the demand boost that European providers need to challenge the hyperscaler oligopoly. Where the lines between levels are drawn, and how strictly they are verified, will therefore decide whether the sovereign market is captured by today's incumbents or opened to European providers.

Article 18 defines the associated third country status that opens Level 3 to providers under third-country control. The Commission may recognise a third country by implementing act where it meets six cumulative criteria: an adequacy decision under the GDPR; no measures allowing it to compel access to non-personal data in conflict with the Data Act; no measures compelling a provider to degrade or disrupt its service or to apply sanctions or embargoes not legitimate under Union or national law; no measures impeding the provision of state-of-the-art technologies; an open market to Union cloud services; and equivalent access to its public procurement.

Article 17 establishes the recognition procedure. A provider applies to the national competent authority of the Member State where it is established. For Level 1 it submits its EU statement of conformity; for Levels 2, 3 and 4 the audit report, a "positive" audit opinion and the evidence given to the auditor. The authority

has 60 days to prepare a draft recognition decision, request further information or reject the application. A draft decision is notified to the authorities of the other Member States, which have 60 days to request clarification or submit a reasoned objection. If none does, the conclusions are "deemed accepted by all Member States" and the service is recognised throughout the Union. If an objection is raised and the evaluating authority maintains its draft, the objecting authority may refer the matter to the Commission, which adopts a binding decision. Statements of conformity issued by SMEs for Level 1 are recognised automatically in all Member States, without review by any authority.

Article 19 provides that Level 1 is self-assessed. The provider carries out a conformity self-assessment without a third-party audit, issues an EU statement of conformity by which it assumes responsibility for compliance, and makes the statement publicly available. The proposal does not say what the statement must contain.

Articles 20 to 22 organise the audits and the register.
Levels 2, 3 and 4 require an independent third-party audit at the provider's expense, by an auditing organisation of the provider's choice that meets independence conditions and has "proven expertise", reviewed every year against the evidence listed in Annex III. Recognised services are registered in a public central repository maintained by the Commission.

Articles 23 and 24 set transparency obligations and penalties.
A recognised provider must notify its auditor and its national authority of any information or material change that may affect its audit or recognition; the authority may then amend or revoke the recognition. Penalties for infringements are laid down by each Member State and must be effective, proportionate and dissuasive; recipients of the services may seek compensation for damage caused by an infringement.

Articles 25 to 28 designate the national competent authorities and organise their cooperation.
Member States designate one or more authorities, which must perform their tasks "in an impartial, transparent and timely manner" and be given sufficient technical, financial and human resources. The authority of the Member State of main establishment has exclusive competence to enforce the framework. Authorities must assist each other and exchange information with the Commission. Where an authority of another Member State suspects that a provider no longer meets Annex II, it may ask the authority of establishment to look into the matter, as may the Commission; the authority of establishment must answer within two months. Neither the authority of another Member State nor the Commission can override the outcome of a recognition by a national authority.

03 / CADA's weakness:

As is, sovereignty will remain unverified

The proposal establishes a needed, auditable baseline for sovereign cloud services across the Union. However, its procedural, governance, and technical provisions contain systemic gaps that could hugely undermine market confidence.

Gaps in CADA

01

Recognition is decided nationally, with limited independence and safeguards against divergence.

Exclusive competence rests with the national authority where the provider chooses its main establishment, while penalties are set nationally without harmonised EU ceilings. Other Member

States can object to initial draft decisions, but the Commission cannot intervene on its own initiative, nor can it override decisions once finalised. Critically, Article 25 does not require competent authorities to be independent of their national governments:

Fragmentation:

similar supply chains will be recognised at different levels, depending on the authority.

A race to the bottom:

providers will establish themselves in jurisdictions where the highest level is easiest to obtain, and Member States will compete to attract them, their jobs, and their investments.

Political influence:

without a guarantee of independence, an assessment conducted by a national authority will be exposed to diplomatic, political or industry pressure.

The Union has seen this before. The one-stop-shop of the GDPR gives the lead to the authority of the Member State of establishment, with the same rule that silence from the other authorities means agreement. The European Parliament concluded that this structure produced geographic imbalances; all nine disputes that escalated to the European Data Protection Board resulted in the lead authority being instructed to revise its draft decision. The GDPR at least obliges the lead authority to escalate a dispute to a collegiate body that decides within a fixed period; that is not the case under CADA.

Overall, without an independent EU authority in charge of implementation, political pressure and lobbying risks diluting enforcement across the board.

02

Level 1 rests on assumption, not demonstration or transparency.

Level 1 is self-declared, and statements issued by SMEs are recognised automatically without any review by an authority. While it is understandable that this level would be weaker, the public statement – the only obligation confirming compliance – can be issued without revealing any information a buyer could use to assess supply chain risks itself. The Commission's own assessment is that "US hyperscalers generally all have offerings that would allow them to qualify under Level 1". Yet Level 1 is the mandatory minimum for the entire public sector, and therefore risks giving public buyers a false sense of protection and control.

03

The framework operates largely behind closed doors.

The Commission must review criteria every 18 months, but the text mandates no structured consultation with industry, technical bodies, or civil society. When amending the Annexes via delegated acts under Article 16, the Commission consults only experts designated by Member States. This lack of external scrutiny limits democratic oversight and deprives regulators of technical market realities.

04

The criteria in Annex II contain ambiguities and loopholes:

- **Too Broad Location Derogations**. At Level 1, infrastructure, assets and data must remain in the Union "unless the public sector body explicitly requires otherwise"; at Levels 2 and 3 the same derogation applies to customer data. The proposal gives no reason for this exception, which reopens the door to third-country access. This is a problem, because in highly concentrated markets, public buyers with low bargaining power can easily be pressured into invoking this waiver.
- **Subcontractor Carve-Outs.** As drafted, the subcontractor scope seems to apply supply chain obligations only to third parties with a "direct contractual relationship" to the provider. A third-country supplier selling through a reseller or an intermediary would escape the subcontractor requirements. Levels 3 and 4 add a further condition – access to classified or sensitive information – which will reduce the scope of subcontractors impacted at the levels meant to be stricter.
- **Source Code Audit Bottlenecks.** Providers at Levels 2 and 3 must subject third-country

software components to source code audits and ensure auditors are granted access. Because access to proprietary source code rests entirely with third-party software vendors, dominant suppliers of proprietary components can selectively grant or withhold audit rights, effectively acting as private gatekeepers determining which European cloud providers achieve Level 2 or 3 recognition.

- **Undefined Terms.** The audits apply to "security-relevant components", a notion the proposal does not define and which does not appear among the definitions of the Cyber Resilience Act to which Annex II refers, and which auditors, providers and authorities may read differently.
- **Ambiguity on Open Source.** It is unclear whether the supply chain measures designed for third-country components also apply to open source software. At Level 4, providers must show that no third-country entity has effective control over a component's design, development, maintenance and evolution. This is difficult to demonstrate for community-governed projects, and the criterion ignores that open source code can be forked and therefore hide such dependency on other open source projects.
- **Inconsistent use of the Cyber Resilience Act definitions.** Annex II cross-references the Cyber Resilience Act's definitions for software bills of materials (SBOMs), components, and manufacturers at Level 2, but inexplicably drops these references at Levels 3 and 4.

05

Associated third country requirements are unclear and inconsistent.

The first Associated third country requirement is "a relevant adequacy decision adopted under Article 45" of the GDPR. The proposal does not say what makes a decision relevant; recital 61 suggests the Commission should look at whether the decision covers the whole country or only certain sectors or certified organisations, and whether it extends to the processing carried out in providing the service, but none of this appears in the article. For example, eleven adequacy decisions in force today were adopted under Directive 95/46/EC and are kept in force by Article 45(9) of the GDPR, on a literal reading, they were not "adopted under Article 45" but only kept in force and recognised by Article 45 or GDPR. Therefore it is unclear if those decisions are in scope.

04 / Our proposed fixes

We make seven recommendations, in three groups. The first guarantees the independence of the authorities that decide whether a service is sovereign. The second opens the framework to transparency: on hardware, at Level 1, and in the review of the levels themselves. The third improves the definitions in Annex II and Article 18.

A. Ensure independent authorities

A.1 Independent authorities and European decision-making to prevent political decisions over technical recognition — Page 14

B. Transparency requirements for the cloud sovereignty framework

B.1 Transparency requirements for hardware (Annexes II and III) — Page 17

B.2 Level 1 transparency requirements for software supply chains (Article 19 and Annex II, point 1) — Page 19

B.3 Transparency of the review and amendment process (Article 16 and second Article 44) — Page 20

C. Improve the definitions in Annex II and Article 18

C.1 Clarify wording, technical aspects and loopholes (Annex II) — Page 21

C.2 Reverse the burden of proof for source code audits (Annex II, points 2.1(i)(ii) and 3.1(i)(ii)) — Page 23

C.3 Clarify the “relevant” adequacy decisions for associated third countries (Article 18) — Page 25

A. Ensure independent authorities

A.1 Independent authorities and European decision-making to prevent political decisions over technical recognition

Technical recognition under the sovereignty framework must be shielded from political, trade and industrial pressure, and must mean the same in every Member State. Independence is necessary but not sufficient: an independent national authority would still decide, for the whole Union, on the providers that chose to establish in its Member State, and that Member State would still compete with the others to attract them. We therefore recommend that the co-legislators give the Union the final say on recognition, through one of three options: an independent European authority, a Commission decision, or independent national authorities whose recognitions the Commission can review.

There are three ways of keeping this decision at EU level, all known to European law:

An independent European authority.

Credit rating agencies were first supervised by their home authority, coordinated through colleges. Because "credit ratings are used throughout the Union", the co-legislators found that structure "not the most appropriate" and gave registration to ESMA, whose decision is "effective for the entire territory of the Union" and whose board must "neither seek nor take instructions" from the Union institutions, any government or any other body. The Court of Justice has confirmed that such powers can be given to a Union body where they call for "specific professional and technical expertise" and are "precisely delineated and amenable to judicial review".

A Commission decision.

The Digital Services Act gives exclusive powers to the Member State of main establishment, as CADA does, except for the largest platforms: given "the challenges involved in effectively supervising them", the Commission designates them after consulting the Member State of establishment and has "exclusive powers" over their systemic risk obligations.[30]

National authorities under Union review.

In the approval of motor vehicles, an authority that finds a type-approval granted by another authority non-compliant "shall refuse to recognise that approval"; if the granting authority objects, the Commission decides by implementing act. The Commission can also act on the results of its own tests, and it periodically assesses the approval authorities. Independence can be guaranteed at national level too: the GDPR requires supervisory authorities to act "with complete independence", and the Cybersecurity Act requires each national certification authority to be "independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making".[31]

Proposed changes:

Option 1 – An independent European authority

01 **European recognition (Articles 17, 25 and 28, new article).**
Entrust the recognition, suspension and withdrawal of recognitions to an independent Union body – ENISA with decision-making powers, or a dedicated authority – with national competent authorities supervising providers on its behalf and sitting on its board.

02 **Independence and appeal (new article).**
Provide that its decision-makers neither seek nor take instructions from any Union institution, government or other body, on the model of Article 42 of Regulation (EU) No 1095/2010, and that its decisions can be challenged before a board of appeal and the Court of Justice.

Option 2 – A Commission decision

01 **Recognition by the Commission (Article 17(5) to (10)).**
Provide that the authority of establishment examines the application and submits a draft decision, and that the Commission adopts the recognition decision by the end of the 60–day review period, taking account of any objection from the authorities of the other Member States.

02 **National enforcement (Articles 25(4), 26 and 28).**
Leave supervision and enforcement with the authority of establishment, and empower the Commission to suspend or withdraw a recognition.

Option 3 – Independent national authorities under a board

01 **Guarantees of independence (Article 25, new paragraphs).**
Provide that competent authorities act free from external influence, neither seek nor take instructions from any government or private body in performing their tasks, have their own staff and budget, and that their management is appointed through a transparent procedure for a fixed term, on the model of Article 52 of Regulation (EU) 2016/679.

02 **Creation of a Sovereignty Authorities Board review before recognition (New Article).**
Create a Board of authorities in charge of enforcing the CADA Cloud Sovereignty Framework and recognise services assurance levels.

03 **Review after recognition (Articles 25(4) and 28).**
Allow the authority of any Member State, or the Commission, to object to a recognition already granted, and provide that the Board adopts a binding decision where the authority of establishment does not withdraw or amend the recognition within one month, as an exception to its exclusive competence.

B. Transparency requirements for the cloud sovereignty framework

B.1 Transparency requirements for hardware (Annexes II and III)

Annex II excludes hardware from the scope of assurance levels and audits. Because Europe and its prospective associated partners currently lack sufficient domestic alternatives for advanced chips and computing hardware, excluding hardware from strict sovereignty mandates is, for now, the pragmatic approach.

However, the framework would nonetheless benefit from a transparency requirement on hardware: providers would disclose the hardware components used to deliver the service – name, function and country of origin – and notify contracting authorities of any change. This would allow authorities to identify problematic dependencies should a new risk emerge, show where Europe's hardware dependencies are deepest, and support the ambition to build supply chains where they are most problematic. Should a European and associated-country supply chain emerge, it could then be rewarded with more trust in the framework. The requirement should take the form of new criteria in Annex II and matching evidence in Annex III.

Proposed changes:

01 **Scope of the Annex (Annex II, introductory paragraph).**
Replace "'Hardware' … is outside of the scope" with a statement that hardware is subject only to the transparency criterion below.

02 **Hardware transparency criterion (Annex II, new point at each level).**
Require the provider to document the hardware components used to deliver the service – name, function, manufacturer and country of origin – and make the list available to the auditing organisation and to the contracting authority.

03 **Notification of changes (Annex II, new point, and Article 23(1)).**
Require the provider to notify contracting authorities of any change in the hardware components used to deliver the service, and treat such a change as a material change for the purposes of Article 23.

04 **Audit evidence (Annex III, new audit criterion).**
List the evidence supporting the hardware transparency criterion: the component inventory, procurement records and the change log.

B. Transparency requirements for the cloud sovereignty framework

B.2 Level 1 transparency requirements for software supply chains (Article 19 and Annex II, point 1)

As discussed previously, the current definition of Level 1 fosters a false sense of security due to its reliance on self-assessment and the absence of clear requirements for the contents of the EU statement of conformity.

To enhance the utility of self-assessment without compromising its practical benefits – particularly for SMEs – co-legislators should explicitly outline both the issuance procedure and required disclosures for the EU statement of conformity. Under this revised framework, providers conducting self-assessments would be required to maintain and publish an up-to-date inventory of all software and hardware components utilised in their services. Furthermore, the Commission should supply a standardised template to define the statement's structure, and the submission process should mandate formal notification
to the designated national competent authority.

/ Proposed changes:

01 **Content of the statement (Article 19(2)).**
Provide that the EU statement of conformity identifies the service, lists the software and hardware components and the subcontractors used to deliver it, and is updated whenever these elements change.

02 **Notification and verification (Article 19(3) and Article 17(3)).**
Require the provider to notify the statement to the national competent authority of establishment, which shall acknowledge that it contains all the required elements, including for statements issued by SMEs, whose automatic recognition in all Member States is otherwise maintained.

B. Transparency requirements for the cloud sovereignty framework

B.3 Transparency of the review and amendment process (Article 16 and second Article 44)

The Union assurance levels form the bedrock of the framework for defining, recognising, and procuring sovereign cloud services. However, Article 16 and the provisions governing delegated acts currently lack adequate mechanisms for democratic oversight and fail to mandate consultation with civil society and technical industry experts.

Amending the Annexes through delegated acts restricts involvement to the European Parliament, the Council, and Member State-designated experts. Furthermore, the review mechanism under Article 16(3) offers no assurances that civil society and industry representatives will be consulted or permitted to highlight implementation challenges.
To ensure comprehensive input, co-legislators should require broad public and stakeholder consultations both prior to any amendments and as part of the review process.

/ Proposed changes:

01 **Annex II review process (Article 16(3)).**
Provide that each review of Annexes II and III includes a public consultation of cloud computing service providers, their customers, auditing organisations and civil society organisations, and that the Commission publishes a report on the outcome.

02 **Stakeholders Consultation before delegated acts (second Article 44(4)).**
Provide that, before adopting a delegated act under Article 16(2), the Commission consults not only experts designated by each Member State but also industry and civil society representatives, through a public consultation of at least eight weeks.

C. Improve the definitions in Annex II and Article 18

C.1 Clarify wording, technical aspects and loopholes (Annex II)

Five points of Annex II need clarification to give providers, auditors and authorities legal certainty and to close the loopholes identified above.

i. "Security-relevant components" (Levels 2 and 3, point (i)(ii)). To give legal certainty on the scope of the source code audits, the co-legislators should define the term: in new recitals giving indications and examples, in Article 2, or in Annexes II and III together with a methodology for identifying the components that are "relevant".

ii. Cyber Resilience Act references (Levels 3 and 4, point (i)). The removal of the references to the Cyber Resilience Act's definitions of software bill of materials, software components and manufacturers at Levels 3 and 4 adds nothing to the assurance provided; the same definitions should be used at all levels.

iii. Open source software. To make clear that the requirements concerning open source software are exclusively those in point (j) of Levels 2, 3 and 4, references to "software" in the supply chain criteria of point (i) should specify "proprietary software" or "software released under a closed source licence". Otherwise, providers relying on open source software cannot know whether the supply chain measures and the vulnerability-reporting requirements apply to open source components.

iv. "Unless the public sector body explicitly requires otherwise". Given the likelihood that dominant third-country providers will press public administrations to use the derogation, the co-legislators should either confine it to a list of cases or delete it. Article 30(4) already allows contracting authorities not to procure a recognised service at all; the derogation is only needed where a contracting authority wants an assurance level but not one of its location elements – for instance for services supporting Member State operations outside the Union's territory.

v. Subcontractors and software intermediaries. The "direct contractual relationship" condition opens a loophole that runs against the purpose of the proposal and overlooks the wide use of software and AI intermediaries on the European market: a third-country manufacturer can enter the supply chain of a recognised service at any level without meeting the requirements against third-country interference and data access, and without its country meeting the Article 18 conditions. The condition should be deleted, or the criteria in the paragraph made non-cumulative.

Proposed changes:

01 **Definition of "security-relevant components" (Article 2, new point; Annex II, points 2.1(i)(ii) and 3.1(i)(ii); Annex III).** Define the term and add to Annex III the methodology by which the provider and the auditing organisation identify the components concerned.

02 **Cyber Resilience Act definitions (Annex II, points 3.1(i) and 4.1(i)).** Reinsert the references to Regulation (EU) 2024/2847, Article 3, points (6), (13) and (39), used in point 2.1(i).

03 **Proprietary software (Annex II, points 2.1(i), 3.1(i) and 4.1(i)).** Specify that the supply chain measures in point (i) concern software released under a proprietary or closed source licence.

04 **Location derogation (Annex II, points 1.1(b), 1.1(c), 2.1(c) and 3.1(c)).** Replace "unless the public sector body explicitly requires otherwise" with a reference to a closed list of cases in which a public sector body may require otherwise, set out in a new point of Annex II, or delete the words.

05 **Subcontractors (Annex II, points 1.2, 2.2, 3.2 and 4.2).** Clarify that the criteria listed are not to be cumulative or delete "that have a direct contractual relationship to the cloud computing service provider" and the condition on access to classified or sensitive information at Levels 3 and 4.

C. Improve the definitions in Annex II and Article 18

C.2 Reverse the burden of proof for source code audits (Annex II, points 2.1(i)(ii) and 3.1(i)(ii))

Beyond the definition of "security-relevant components", we invite the co-legislators to consider carefully the effect of the source code audits, on a market defined by high concentration and by components in some cases supplied almost exclusively by third-country manufacturers.

As worded, the obligation falls on the cloud provider, not on the third-country manufacturer of the component: Annex III requires the audited provider to "ensure that the third-party independent auditor is granted the right to access and audit the source code". If a component provider refuses access to a proprietary component's source code, the European provider has no way to comply. In practice, manufacturers of components with little or no alternative become the kingmakers deciding if services can be recognised at Levels 2 and 3.

We call on the co-legislators to correct this through one of the three options below, so that dominant component suppliers cannot combine market position, its intellectual property rights and audit refusal.

Proposed changes:

01 **Option 1 –**
Reference to the European scheme (Annex II, points 2.1(i)(ii) and 3.1(i)(ii)).
Remove the source code audit as such and refer instead to the source code requirements of the European cybersecurity certification scheme covering cloud computing services, as the means of ensuring the absence of a kill switch.

02 **Option 2 –**
Obligation on manufacturers (new article in Section 3; Annex III, audit criterion I).
Require manufacturers of software components
used to deliver a service undergoing an audit under Article 20 to grant the auditing organisation access to the source code of security-relevant components, under confidentiality, within a defined period.

03 **Option 3 –**
Register of component audits (Article 22, new paragraph).
Require the Commission to maintain in the central repository a register of source code audits of third-country components, whose results are available to all cloud computing service providers established in the Union and to national competent authorities, and provide that a component already audited need not be audited again by each provider.

C. Improve the definitions in Annex II and Article 18

C.3 Clarify the "relevant" adequacy decisions for associated third countries (Article 18)

As it stands, Article 18 is unclear on the notion of a "relevant" adequacy decision for associated third country status. And it refers to decisions "adopted under Article 45" of the GDPR, although eleven of the adequacy decisions in force (i.e. Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay) were adopted under Article 25(6) of Directive 95/46/EC and are kept in force under the GDPR. The Commission reviewed them in January 2024 and concluded that each "continues to ensure an adequate level of protection". On a literal reading, Decisions 2000/518/EC (Switzerland), 2004/411/EC (Isle of Man) or 2011/61/EU (Israel) would not qualify.

We invite the co-legislators to define what "relevant" means – the test already sketched in recital 61 is a good starting point – and to confirm that adequacy decisions adopted before the GDPR and still in force count for
the purposes of Article 18.

Proposed changes:

01 **Pre-GDPR decisions (Article 18(1)(a)).** Replace "adopted under Article 45 of Regulation (EU) 2016/679" with "adopted under Article 45 of Regulation (EU) 2016/679 or remaining in force pursuant to Article 45(9) of that Regulation".

02 **Meaning of "relevant" (Article 18(1)(a)).** Specify that an adequacy decision is relevant where it applies to the third country as a whole, or where its scope covers the processing activities carried out in the provision of the cloud computing services concerned.

Sources and resources

1. European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final, 2026/0138 (COD), 3 June 2026. https://ec.europa.eu/newsroom/dae/redirection/document/129111
2. European Commission, Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 502 final, Part 1/2, 3 June 2026, p. 25. https://ec.europa.eu/newsroom/dae/redirection/document/129113
3. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, pp. 80–81.
4. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 25, footnote 85.
5. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 24.
6. COM(2026) 502 final (CADA proposal), as above, recital 48, p. 27.
7. COM(2026) 502 final (CADA proposal), as above, recital 47, p. 26.
8. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, pp. 14 and 25.
9. European Commission, "Sovereign Cloud Framework explained", news item, 1 June 2026. https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en
10. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 5, footnote 5.
11. European Commission, Report from the Commission to the European Parliament and the Council on the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework, COM(2026) 9 final, 20 January 2026 (Council document 5565/26), pp. 8–9. https://data.consilium.europa.eu/doc/document/ST-5565-2026-INIT/en/pdf
12. European Commission, Annexes 1 to 3 to the proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final, 3 June 2026, pp. 5, 7 and 9. https://ec.europa.eu/newsroom/dae/redirection/document/129112
13. COM(2026) 502 final, Annexes 1 to 3, as above, p. 4.
14. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 40.
15. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 46.
16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Articles 56(1) and 60(6). http://data.europa.eu/eli/reg/2016/679/oj
17. European Parliament, Resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, P9_TA(2021)0111, paragraphs 19 to 21. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021IP0111
18. European Commission, Communication from the Commission to the European Parliament and the Council – Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, 25 July 2024, section 2.2. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0357
19. Regulation (EU) 2016/679 (GDPR), as above, Articles 60(4), 65(1)(a) and 65(2).
20. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 40.
21. COM(2026) 502 final (CADA proposal), as above, Article 16(2) and (3), p. 51, and second Article 44(4), p. 72.
22. COM(2026) 502 final, Annexes 1 to 3, as above, pp. 4, 5 and 7.
23. COM(2026) 502 final, Annexes 1 to 3, as above, pp. 4, 6, 8 and 10.
24. COM(2026) 502 final, Annexes 1 to 3, as above, pp. 6, 8 and 21.
25. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), Article 3. http://data.europa.eu/eli/reg/2024/2847/oj
26. COM(2026) 502 final, Annexes 1 to 3, as above, pp. 6, 8 and 9.
27. COM(2026) 502 final (CADA proposal), as above, Article 18(1)(a), p. 53, and recital 61, pp. 29–30.
28. European Commission, Report on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM(2024) 7 final, 15 January 2024, section 1 and footnote 15. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0007
29. COM(2026) 502 final (CADA proposal), as above, recital 59 and Article 25(3), pp. 29 and 58.
30. Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies, Articles 14(2), 15(1) and 16(3), as amended. http://data.europa.eu/eli/reg/2009/1060/oj ; Regulation (EU) No 513/2011 of the European Parliament and of the Council of 11 May 2011 amending Regulation (EC) No 1060/2009 on credit rating agencies, recitals 6 and 8. http://data.europa.eu/eli/reg/2011/513/oj ; Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Article 42. http://data.europa.eu/eli/reg/2010/1095/oj ; Court of Justice, judgment of 22 January 2014, United Kingdom v European Parliament and Council of the European Union, C-270/12, EU:C:2014:18, paragraph 53. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0270 ; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act), Articles 33(4) and 56(1) and (2). http://data.europa.eu/eli/reg/2022/2065/oj
31. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, Articles 9, 10 and 54. http://data.europa.eu/eli/reg/2018/858/oj ; Regulation (EU) 2016/679 (GDPR), as above, Article 52(1).
32. COM(2026) 502 final, Annexes 1 to 3, as above, p. 4.
33. COM(2026) 502 final (CADA proposal), as above, second Article 44(4), p. 72.
34. COM(2026) 502 final, Annexes 1 to 3, as above, p. 21.
35. Regulation (EU) 2016/679 (GDPR), as above, Article 45(9); COM(2024) 7 final (review of the adequacy decisions adopted under Directive 95/46/EC), as above, section 1.
36. COM(2024) 7 final (review of the adequacy decisions adopted under Directive 95/46/EC), as above, section 4.
37. Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000D0518
38. Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004D0411
39. Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011D0061

FOTI