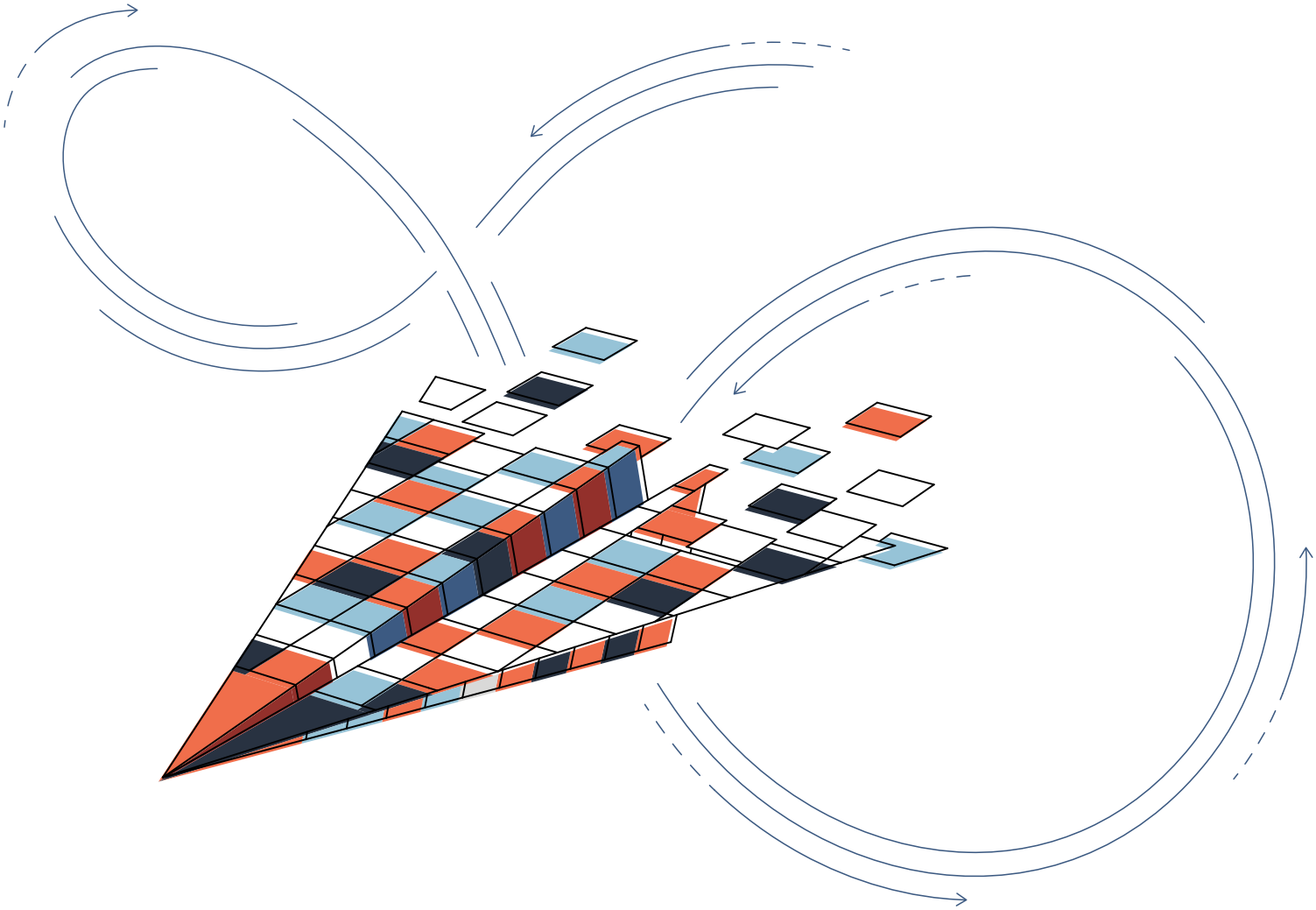
The Cloud and AI Development Act Proposal

Extensive Regulation for Limited Sovereignty Gains?



Dr. Zuzanna Warso & Dr. Kristina Irion

November 2026

Executive summary

Throughout the EU, there is a clear political ambition to use public procurement as a lever to reduce reliance on a small number of non-EU cloud service providers and to open the market to a wider range of providers. The European Parliament stressed 'the importance of leveraging public procurement to support the deployment and scaling of open and interoperable digital solutions' and called for 'reducing reliance on single providers'.[1] There is a growing number of public sector initiatives migrating their services away from the three US hyperscalers.[2]

The Commission's Communication on European Tech Sovereignty acknowledges that procurement practices tend to 'favour incumbent suppliers and tolerate vendor lock-in', and presents its proposal for a Cloud and AI Development Act (CADA) as a way to 'decrease overreliance on certain providers'.[3] Yet, as the CADA proposal is designed, it is more **likely to preserve the status quo** than to enable public procurement to be used to scale up an open source and interoperable European digital stack.

In this report, we examine Title IV of the CADA proposal entitled 'Autonomy' covering new rules for:

- a cloud computing sovereignty framework with its four Union assurance levels, and
- risk assessments and public procurement of cloud computing services used by public sector bodies in the Member States and Union entities.

In examining these rules, we identified the following issues:

The regulatory architecture of Title IV

- Although the CADA proposal frames reliance on third-country cloud providers as a question of sovereignty, it addresses that reliance through the logic and mechanisms of information security risk regulation.
- By linking higher sovereignty requirements to a public sector activity's contribution to *the preservation of public order*, the CADA proposal risks limiting the ability of public sector bodies to use procurement strategically to strengthen European digital infrastructure and promote European cloud providers.
- Article 30(2) could be interpreted as requiring public authorities to procure Union assurance level 1 services for activities that do not contribute to the preservation of

---

[1] European Parliament resolution of 22 January 2026 on European technological sovereignty and digital infrastructure (2025/2007(INI)), paras 32 and 68, ELI: http://data.europa.eu/eli/C/2026/3697/oj.

[2] See the timeline of such initiatives compiled by WIRED reporter Matt Burgess at <https://public.flourish.studio/visualisation/29262259/?full> (accessed 25 October 2026).

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy ('Communication on European Tech Sovereignty'), COM(2026) 503 final, Brussels, 3 June 2026, 10 (fn 55) and 24 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026DC0503 (accessed 25 October 2026).

public order, thereby limiting their discretion to demand higher sovereignty levels. Rather than establishing a minimum standard, the framework risks creating a ceiling on sovereignty requirements.

- The CADA proposal would give the Commission the final say over which Union assurance levels apply to which type of public sector activities, and over disputes between national authorities on the recognition of providers.

- Once adopted, CADA would pre-empt Member State initiatives on cloud sovereignty that differ from harmonised EU law, including initiatives that aim to reduce dependency on the three US hyperscalers, which control more than 70 percent of the Union's cloud market.

Supply side and governance

- Recognising third-country control over cloud computing service providers established in the Union would be a step in the right direction compared with the EUCS. However, Union assurance level 2 would still leave room for 'sovereign cloud' arrangements involving US hyperscalers.

- Union assurance level 3 generally excludes third-country control, but the exception for 'associated third countries' leaves open the possibility that the Commission recognises a third country after the CADA is adopted.

- Annex II restricts the use of service-generated data for AI training by third-country actors but does not explicitly extend this prohibition to all customer data, nor does it expressly restrict providers' own use of customer data for AI training within the EU. The broader wording of Annex III creates uncertainty about the intended scope of the safeguard.

- The CADA proposal addresses technological dependencies in software but expressly excludes hardware from the sovereignty assessment, even though software and hardware dependencies are closely interconnected.

- Recognition at Union assurance levels 2 to 4 relies heavily on evidence provided by cloud service providers themselves, raising questions about auditors' ability to independently identify and verify information that providers do not disclose.

- The CADA proposal does not require national competent authorities responsible for recognition and supervision to be institutionally independent, despite the significance of their decisions for the application of the sovereignty framework.

- The EU-wide consistency mechanism is entrusted to the Commission rather than a board of independent regulatory authorities, raising questions about the institutional independence of oversight and the concentration of powers in the Commission.

Demand side: risk assessments and public procurement

- The meaning of a public sector activity contributing to 'the preservation of public order' (Article 29(1)(a)) is not defined. As this is an important legal threshold in the

CADA for the risk assessments of public sector activities it should also be defined in the legislation.

- The CADA proposal's legal threshold of contributing to 'the preservation of public order' effectively excludes public sector activities at Union assurance level 1 (circa 70 percent) from being assessed following the risk assessment criteria in Article 29(2).
- It would be a missed opportunity not to build 'European preference requirements' into CADA in relation to cloud computing services at Union assurance levels 1 and 2 to reduce dependencies, increase supply chain security and economic security more broadly.
- This detailed regulatory framework could be used by cloud service providers to challenge public sector bodies and contracting authorities in the Member States and Union entities whenever they deviate ever so slightly from the Union assurance levels.
- Three additional measures to enhance resilience and limit dependency – a multi-vendor/-cloud strategy, Union added value and open standards – may together steer public procurement by Member States' public sector bodies and Union entities towards improved sovereignty and better resilience; yet the scope and reach of these measures are limited or optional.

As it stands, the CADA risks creating an extensive legal framework while delivering only limited gains in sovereignty. We therefore propose a set of recommendations to address the proposal's shortcomings and avoid this outcome.

Table of Contents

Executive summary ***1***

1. Introduction ***5***

2. The regulatory architecture of Title IV 'Autonomy' ***6***

2.1. Services covered by the cloud computing sovereignty framework 6

2.2. Two-sided regulatory framework for cloud computing services' supply and demand 7

2.3. Cloud sovereignty becomes information security risk regulation 7

2.4. The Commission as rule-setter and arbiter 8

2.5. EU law pre-emption of Member States' digital sovereignty ambitions 9

2.6. Key issues 10

3. Supply-side measures: the cloud computing sovereignty framework ***11***

3.1. Third-country control and operational autonomy 11

3.2. Data sovereignty 13

3.3. Technological dependencies 14

3.4. The governance structure: independent auditors but not independent authorities 16

3.5. Key issues 17

4. Demand-side measures ***18***

4.1. Risk assessments of public sector activities 18

4.2. Public procurement of cloud computing services 24

4.3. Additional measures to enhance resilience and limit dependency 28

4.4. Key issues 29

5. Conclusions and recommendations ***30***

About this report ***34***

1. Introduction

In early June 2026, the European Commission ('the Commission') released the European Technological Sovereignty Package.[4] The package brings together several measures to strengthen Europe's capacity in semiconductors, artificial intelligence (AI), cloud computing and open source. One of these measures is the proposal for a Cloud and AI Development Act (CADA).[5] The CADA proposal covers three main areas: 'Research, Development and Deployment Activities for the Cloud and AI Ecosystem' (Title II), 'Data Centre Capacities' (Title III), and 'Autonomy' (Title IV).

The Explanatory Memorandum accompanying the proposal notes that 'three non-EU hyperscalers control over 70% of the European cloud market' and that '[w]hile the EU market for cloud computing services [...] is growing significantly, the market share of EU providers decreased from 29% in 2017 to 15% in 2022'.[6] The Communication on European Tech Sovereignty estimates that '[t]he EU currently spends EUR 264 billion a year mostly on US proprietary IT products and services.'[7] Against this background, Title IV on 'Autonomy' of the CADA proposal introduces a 'Union cloud computing sovereignty framework determining criteria for trusted cloud computing services'[8] and corresponding rules for assessing public sector activities and procuring cloud computing services.

This report examines the mechanism set up in Chapter I ('Cloud computing sovereignty framework') and Chapter II ('Demand side measures') of Title IV in light of the objective to enhance the EU's digital sovereignty. It asks what the measures are likely to mean for the digital sovereignty of cloud-based activities of public sector bodies in the Member States and Union entities. The analysis does not cover Title II on 'Research, Development and Deployment Activities for the Cloud and AI Ecosystem' or Title III on 'Data Centre Capacities'.

The report is structured as follows. Section 2 sets out the regulatory architecture underpinning Title IV, examining how the proposal operationalises the concept of sovereignty and how it distributes powers between Member States and the Commission. Section 3 analyses the cloud computing sovereignty framework and its four Union assurance levels, while Section 4 examines the demand-side measures of the framework, focusing on public sector risk assessments and procurement of cloud computing services intended for public sector activities. The final section sets out recommendations.

---

[4] Communication on European Tech Sovereignty (n 3), 16.

[5] 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, Brussels, 3 June 2026 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0502> (accessed 25 October 2026).

[6] Explanatory Memorandum to the CADA proposal (n 5), 1.

[7] Communication on European Tech Sovereignty (n 3), 16.

[8] Recital 51 CADA proposal.

2. The regulatory architecture of Title IV 'Autonomy'

The CADA proposal establishes 'a framework for strengthening the cloud and AI ecosystem at Union level.'[9] It pursues two objectives. The first objective is to ensure the conditions necessary for the competitiveness and innovation capacity of the EU's cloud and AI ecosystem.[10] The second is to increase the EU's resilience and strategic autonomy in cloud and AI technologies.[11] The proposal lists several measures through which it establishes the framework, including enabling 'the availability of a sovereign cloud and artificial intelligence (AI) offer to safeguard the Union's public order' and reducing 'dependencies on critical technologies'.[12] The Explanatory Memorandum sheds more light on these measures and states that the CADA proposal aims to mitigate 'the risks stemming from the EU's reliance on third countries for cloud computing services via a single EU-wide sovereignty framework.'[13] Yet, the CADA proposal does not define key notions such as 'sovereignty', 'resilience', 'strategic autonomy' or 'public order'.[14] CADA's conception of cloud sovereignty therefore has to be reconstructed from the regulatory mechanisms it establishes, which is the focus of this section.

2.1. Services covered by the cloud computing sovereignty framework

The notions of cloud computing service, cloud computing service providers, Union entities and public sector bodies used in Chapters I and II of Title IV are defined at the beginning of the CADA proposal.[15] Cloud computing service is defined through a reference to the NIS2 Directive as 'a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations.'[16]

While Chapter I does not explicitly mention AI systems or agents in its operative text and Chapter II mentions AI systems only in its procurement award and monitoring provisions,[17] recital 10 clarifies that on-demand access to AI systems, in the sense of their delivery and

---

[9] Article 1(1) CADA proposal.

[10] Article 1(2) CADA proposal.

[11] Article 1(3) CADA proposal.

[12] Article 1(2)(c) and (d) CADA proposal.

[13] Explanatory Memorandum to the CADA proposal (n 5), 2.

[14] Rhetorically, these terms are very prevalent in the text of the CADA proposal and its annexes: sovereignty (18)/ sovereign (4), autonomy (19), resilience (25)/ resilient (9), public order (19).

[15] Article 2(1), (2), (6) and (7) CADA proposal.

[16] Article 6, point (30), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive), consolidated text <http://data.europa.eu/eli/dir/2022/2555/2022-12-27> (accessed 25 October 2026).

[17] Articles 32 and 33 CADA proposal.

making available, is covered by the definition of cloud computing services. What is excluded from the definition is the AI system itself and its underlying model.

2.2. Two-sided regulatory framework for cloud computing services' supply and demand

For cloud computing services offered to public sector bodies and Union entities, the CADA proposal translates its objectives related to sovereignty into a two-sided regulatory framework:

On the supply side, it establishes four Union assurance levels against which all cloud computing service providers are assessed.[18] Providers under the control of a third country are allowed at level 1, can supply services at level 2 subject to certain safeguards, are excluded from level 3 unless the third country is recognised as an 'associated third country', and are prohibited at level 4. Providers seeking recognition at levels 2 to 4 must undergo an independent audit.

On the demand side, Member States' public sector bodies and Union entities conduct risk assessments to determine which assurance level is appropriate for particular public sector activities. The two sides come together in public procurement, where contracting authorities must procure cloud services at the assurance level determined through the risk assessment.[19] In Sections 3 and 4 we explain in more detail the two sides of the framework and how they work together.

2.3. Cloud sovereignty becomes information security risk regulation

While the CADA proposal frames Europe's reliance on third-country cloud providers as a question of sovereignty and autonomy, when it comes to public procurement it addresses that reliance using the logic and mechanisms of information security risk regulation. The proposal's approach builds on EU cybersecurity and cloud assurance levels including the European Cybersecurity Certification Scheme for Cloud Services (EUCS) proposed by the EU Agency for Cybersecurity (ENISA). A direct precedent is the Commission's 2025 Cloud Sovereignty Framework, which includes the Sovereignty Effectiveness Assurance Levels (SEALs) to assess cloud services offered to EU institutions and bodies.[20]

The threshold for determining when reliance on third-country cloud providers warrants higher sovereignty requirements is whether the public sector activity contributes to the 'preservation of public order.'[21] The proposal confines this test to activities in sectors falling

---

[18] Articles 16-28 and Annexes II and III CADA proposal.

[19] Article 30 CADA proposal.

[20] European Commission, 'Sovereign Cloud Framework explained', News article, 1 June 2026, <https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en> (accessed 25 October 2026).

[21] Article 29(1)(a) CADA proposal.

under Annexes I and II of the NIS2 Directive[22] and in 'the areas of national security, internal security, external border management, defence, justice or law enforcement'.[23] The security-infused approach is also reflected in the Commission's Communication on European Tech Sovereignty, which places CADA alongside the Open Source Strategy as building on the proposed revision of the Cybersecurity Act.[24]

As a result of this risk-based approach, the required degree of cloud sovereignty is tied to the criticality of the public sector activity to which the risk-based measures apply. On the one hand, such a regulatory approach could level up the information security of public sector activities hosted in the cloud in Member States where this has not yet been addressed. On the other hand, it also suggests that the CADA would not allow public procurement to be leveraged more broadly and strategically to promote the uptake of EU-native cloud services and thereby reduce dependencies on non-EU providers beyond the small share of highly critical public sector activities. Strategic public procurement of the kind proposed by the EuroStack initiative, Dutch digital regulators and the European Parliament's resolution on European technological sovereignty and digital infrastructure might effectively be limited by the CADA proposal's operationalisation of sovereignty as risk regulation.[25] We come back to this issue in Section 4 below.

2.4. The Commission as rule-setter and arbiter

Title IV of the CADA proposal would give the Commission significant competences to shape and supervise which Union assurance levels apply to the cloud computing services used by Member States' public sectors. Day-to-day application of Title IV would remain largely with Member States: national competent authorities would recognise and supervise providers, and Member States and Union entities would carry out the risk assessments of their public sector activities. The Commission, however, would adopt delegated and implementing acts and decisions, review and amend the annexes, issue methodologies, forms and guidance, settle disputes between national competent authorities, and review and, where necessary, override Member States' risk assessments. Through the CADA, the Commission would

---

[22] NIS2 Directive (n 16). The NIS2 Directive establishes cybersecurity risk-management and reporting obligations for entities in sectors of high criticality listed in Annex I which covers inter alia public administration and other critical sectors listed in Annex II. Many of the entities regulated by NIS2 are private activities such as energy, transport, banking, financial market infrastructures, health, drinking water and wastewater, digital infrastructure, ICT service management, postal services, waste management, chemicals, food, manufacturing, digital providers and research.

[23] Article 29(1)(a) CADA proposal.

[24] Communication on European Tech Sovereignty (n 3), 5: 'The CADA and the open source strategy build on the framework developed by the proposed revision of the EU Cybersecurity Act, which creates a certification and risk-management framework that can effectively limit the role of high-risk vendors in critical digital infrastructures.'

[25] EuroStack, 'A Proposed Framework for a "Buy European" Regulation of Strategic Digital Procurement', 29 September 2025, <https://eurostack.eu/wp-content/uploads/2025/09/buy-european-a-framework-for-strategic-procurement-29-september-25.pdf> (accessed 25 October 2026); Authority for Consumers and Markets et al, 'Towards digital autonomy: Increased control over digital dependencies', 10 July 2026 <https://www.acm.nl/system/files/documents/towards-digital-autonomy.pdf> (accessed 25 October 2026); European Parliament resolution (n 1).

become the rule-setter and final arbiter of a framework that treats cloud 'sovereignty' across the entire public sector as a matter of risk regulation.[26]

The proposal therefore goes beyond setting common standards for Member States to apply. Certain decisions **with a significant impact on the scope and depth of the information security the CADA would offer,** such as **specifying when public services contribute to the 'preservation of public order' or recognising 'associated third countries', will be made by the Commission after the proposal's adoption.** Moreover, the numerous implementing acts and decisions envisaged by the proposal suggest that the resulting regulatory framework could become extensive and detailed, in contrast to the regulatory simplification the Commission champions elsewhere.

2.5. EU law pre-emption of Member States' digital sovereignty ambitions

The EU legislative competence to pass the CADA proposal is primarily based on the shared competence to harmonise Member States' laws for the establishment and the functioning of the internal market.[27] According to its settled case-law, the Court of Justice of the European Union (CJEU) holds that where EU legislation fully harmonises a particular field, a Member State cannot adopt national rules which are more restrictive, more detailed or different to EU legislation put in place in the 'occupied' field.[28]

Several provisions of Title IV indicate that the CADA proposal establishes a fully harmonised framework for determining public sector cloud computing sovereignty requirements.[29] **CADA would thus pre-empt the adoption of national measures imposing additional cloud sovereignty requirements.**[30]

Importantly, according to Article 30(2), public authorities 'shall use' cloud computing services having Union assurance level 1 for activities that do not contribute to the preservation of public order. This suggests that the CADA proposal does not merely establish common minimum standards but also limits Member States' discretion to require higher sovereignty levels. **In other words, rather than creating a sovereignty floor, it creates a sovereignty**

---

[26] E.g. Articles 16(2) and (3), 17(10) and (12), 18, 20(9), 21(1), 28(2), 29(3) and (5), 31(2) and (3) CADA proposal.

[27] Article 114(1) of the Treaty on the Functioning of the European Union (TFEU) (consolidated version), OJ C 202, 7.6.2016, 42–43. The proposal also mentions the competitiveness of the Union's industry as a legal basis which however does not allow for the harmonisation of Member States' laws, Article 173(3) TFEU.

[28] Case 148/78 (*Criminal Proceedings against Tullio Ratti*) EU:C:1979:110, paras 26-27. See Michèle Finck, 'Legal Imaginations of the AI Act: A Constitutional Perspective on the Pre-Emption of Member State Competence' (2026) 63 Common Market Law Review, <https://doi.org/10.54648/cola2026067> (accessed 25 October 2026).

[29] See the list of implementing regulations and decisions delegated to the Commission in fn 26.

[30] Robert Schütze, 'EU Competences' in Damian Chalmers and Anthony Arnull (eds), *The Oxford Handbook of European Union Law* (OUP 2015) 86; Stephen Weatherill, 'The Fundamental Question of Minimum or Maximum Harmonisation' in Sacha Garben and Inge Govaere (eds), *The Internal Market 2.0* (Hart Publishing 2022) 265.

ceiling.[31] At this stage, it is important to establish whether the CADA proposal would become an obstacle for the growing number of public sector initiatives in the Member States that aim for digital sovereignty and deliberately shift their demand away from the three US hyperscalers that currently control over 70% of the European cloud market.[32]

2.6. Key issues

- Although the CADA proposal frames reliance on third-country cloud providers as a question of sovereignty, it addresses that reliance through the logic and mechanisms of information security risk regulation.

- By linking higher sovereignty requirements to a public sector activity's contribution to the preservation of public order, the CADA proposal risks limiting the ability of public sector bodies to use procurement strategically to strengthen European digital infrastructure and promote European cloud providers.

- In particular, Article 30(2) could be interpreted as requiring public authorities to procure Union assurance level 1 services for activities that do not contribute to the preservation of public order, thereby limiting their discretion to demand higher sovereignty levels. Rather than establishing a minimum standard, the framework risks creating a ceiling on sovereignty requirements.

- The CADA proposal would give the Commission the final say over which Union assurance levels apply to which type of public sector activities, and over disputes between national authorities on the recognition of providers.

- Once adopted, CADA would pre-empt Member State initiatives on cloud sovereignty that differ from harmonised EU law, including initiatives that aim to reduce dependency on the three US hyperscalers, which control more than 70 percent of the Union's cloud market.

---

[31] The Explanatory Memorandum describes level 1 as a minimum requirement ('Article 30 sets out obligations for contracting authorities that procure cloud computing services to procure, as a minimum requirement, Union assurance level 1.'), which could suggest that public authorities remain free to require higher assurance levels. However, this is not reflected in the wording of Article 30(2), which does not expressly allow authorities to exceed the prescribed level, rather the opposite.

[32] See the timeline compiled by WIRED reporter Matt Burgess (n 2).

3. Supply-side measures: the cloud computing sovereignty framework

The CADA proposal establishes four Union assurance levels which become stricter the higher the level. For each criterion, Annex II specifies the requirements that providers must meet at each assurance level. Table 3 at the end of this report summarises the main requirements and shows how they differ across the four assurance levels. Most of these criteria protect the confidentiality, integrity and availability of data and services against interference by third countries or entities established there.

The focus of this section is on selected criteria that are particularly relevant to CADA's stated objective of mitigating the EU's reliance on third-country cloud providers. We examine the key distinctions between the different Union assurance levels and whether and how the requirements reduce underlying dependencies and promote resilience. We then explore some challenges related to the process for seeking recognition.

3.1. Third-country control and operational autonomy

One of the most important distinctions between the different assurance levels concerns control over the provider of cloud services by entities established in third countries.[33] Similarly to the Commission's Cloud Sovereignty Framework,[34] the CADA proposal recognises that such control may expose providers to third-country jurisdiction and risks of third-country interference. **Recognising third-country control over cloud computing service providers established in the Union certainly is a step forward from the EUCS.**[35]

As a general rule, third-country control is permitted at assurance level 1 and, subject to safeguards, also at assurance level 2. More specifically, at level 2 the provider must put in place legal, technical and organisational measures to prevent that control from affecting the provision of the service. Among other things, these measures must prevent third-country access to customer data and the possibility of disruption or degradation of the service.[36] In other words, level 2 seeks to *manage* the risks arising from third-country control of the service provider, rather than *eliminate* such control. **In practical terms, level 2 leaves room**

---

[33] 'Control' is defined by reference to Article 2(6) of Regulation (EU) 2021/697 which defines control as 'the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities.' Third-country control can be exercised either by a third country itself or by a legal entity established in a third country. Annex II, criterion (g) CADA proposal. Annex III operationalises this test by requiring auditors to examine ownership structures and specific rights, corporate governance, commercial and financial links, and other possible sources of control. Annex III, 7–7.1 CADA proposal.

[34] European Commission, Cloud Sovereignty Framework – Implementation Guidance <https://commission.europa.eu/document/download/2ad80a48-166f-4c77-a513-80c53ca2a128_en?filename=Cloud+Sovereignty+Framework+-+Implementation+guidance.pdf> (accessed 25 October 2026).

[35] The EU Cybersecurity Certification Scheme for Cloud Services (EUCS) is a certification scheme pursuant to the Cybersecurity Act (CSA). The 'absence of foreign jurisdiction' requirement had been controversially discussed and delayed the adoption of the EUCS, see Luca Bertuzzi, 'Netherlands gathers opposition front to EU cloud certification scheme', Euractiv, 7 December 2023.

[36] Annex II, 2.1(g) CADA proposal.

for 'sovereign cloud' arrangements involving US hyperscalers. The Impact Assessment mentioned 'sovereign joint ventures' as one of the arrangements likely to qualify at this level,[37] which are increasingly formed by US hyperscalers.[38] A relevant precedent is the Commission's sovereign cloud procurement framework of up to €180 million under which one of the contracts was awarded to a Proximus-led consortium that uses services from S3NS, a joint venture between Thales and Google Cloud.[39]

Third-country control is prohibited at both levels 3 and 4. However, at level 3, a provider controlled from a third country may still qualify if that country has been designated by the Commission as an 'associated third country'.[40] At this point, it is unclear which countries could qualify for this designation. In correspondence with the authors, the Commission confirmed that any third country meeting the cumulative criteria under Article 18 could in principle qualify. While the US appears unlikely to meet all of these criteria, particularly in light of the CLOUD Act, the Commission still has to make that assessment.[41] **The possibility that US-controlled providers qualify for level 3 therefore cannot be ruled out,** albeit that would appear outlandish at this moment.[42]

Third-country control is not the only way in which actors outside the EU can influence the provision of a cloud service. The CADA proposal also looks at whether technical and operational support is provided from outside the EU and whether third-country subsidiaries can access EU customer data, privileged accounts[43] or otherwise interfere with the EU operation.[44] In this sense, the framework looks beyond formal establishment and corporate control to the operational autonomy of the service. Finally, control can change over time, for example through an acquisition or changes in the provider's ownership or governance structure. The CADA proposal requires recognised providers to report any material change in circumstances that may affect their recognition.[45] Following such a notification, the auditor

---

[37] Commission Staff Working Document, Impact Assessment Report Accompanying the document 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) (Impact Assessment), SWD(2026) 502 final, 40.

[38] Rafael Grohmann and Alexandre Costa Barbosa, 'Sovereignty-as-a-service: How big tech companies co-opt and redefine digital sovereignty', (2026) Media, Culture & Society 48(2), 416-424. https://doi.org/10.1177/01634437251395003.

[39] European Commission, 'Commission advances cloud sovereignty through strategic procurement', 17 April 2026 <https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en> (accessed 25 October 2026).

[40] Article 18; Annex II, 3.1(g) CADA proposal.

[41] Article 18 CADA proposal.

[42] Note that the Commission has adopted three successive adequacy decisions for the US: on the Safe Harbour principles and on the Privacy Shield, both under Directive 95/46/EC and both invalidated by the CJEU, and currently on the EU–US Data Privacy Framework under the GDPR. Each recognises an adequate level of protection for US organisations certified under the respective framework.

[43] 'Privileged accounts' refer to administrative or superuser credentials, such as Identity and Access Management (IAM), database administration, and security operations roles, that grant elevated technical control over cloud infrastructure. Annex III, criterion (k) CADA proposal.

[44] Annex II, criteria (h) and (k); Annex III, 8 and 11 CADA proposal.

[45] Article 23(1) CADA proposal.

and the competent authority must assess whether the audit opinion or recognition needs to be amended or revoked.[46]

3.2. Data sovereignty

CADA's approach to data sovereignty extends beyond geographic localisation. The framework establishes a distinction between where customer data is stored and processed and how operational and usage data can be processed or re-used.

3.2.1. Data localisation

For levels 1 to 3, all customer data, including metadata and telemetry, processed, stored and transferred by the provider or its subcontractors, must remain exclusively within the EU, unless the public sector customer explicitly requests an exception.[47] For level 4, localisation becomes absolute for customer data classified as sensitive, with no public sector opt-out.[48]

3.2.2. Restrictions on using customer data for AI training

In addition to data localisation, from level 2 onwards Annex II introduces an additional safeguard prohibiting the use of 'data generated by using the audited service' to train or fine-tune AI systems operated by a third country or third-country entity and the transfer of such data outside the EU.[49]

While this criterion addresses an important risk, namely the use of data for AI training, it is unclear why the safeguard is limited *to the data generated by using the audited service* and does not apply to all customer data (which in this case is that of a public body stored and processed by the provider). Annex II leaves input and stored customer data governed primarily by criterion (c) (localisation), without an explicit prohibition under criterion (f) regarding AI training. In other words, nothing in Annex II stops the provider itself from training AI on customer data, as long as the data stays within the EU and is not personal data covered by the GDPR. For non-personal data, any such restriction would currently have to come from the contract with the public sector body. Criterion (g)(ii) does not fill that gap: at levels 2 and 3, it only requires providers controlled by a third country or third-country entity to prevent access to customer data by that third country or entity, not to refrain from using it themselves, e.g. for AI training.

There is also a discrepancy between the substantive requirement related to the AI training in Annex II and the corresponding evidence listed in Annex III. While Annex II refers only to 'data generated by using the audited service', Annex III indicates that the auditors should examine evidence concerning data '*processed* or generated by using the audited service', including customer-derived data, logs and telemetry and that they should look at contractual clauses specifying that data are processed solely for the delivery of the audited service and not for

[46] Article 23(2) and (3) CADA proposal.

[47] Annex II, 1.1(c), 2.1(c), 3.1(c) CADA proposal.

[48] Annex II, 4.1(c) CADA proposal.

[49] Annex II, 2.1(f), 3.1(f), 4.1(f) CADA proposal.

any secondary purposes.[50] It is unclear whether the broader wording is meant only to guide the collection of evidence or to reflect the intention to extend the safeguard to all customer data.

3.3. Technological dependencies

The CADA proposal introduces software supply chain measures to address dependencies on software that is provided, owned or licensed by third-country entities.[51] There are no equivalent guarantees regarding hardware.[52]

3.3.1. Software

The requirements related to the software supply chain begin at level 2, although level 1 already requires providers controlled by a third country to guarantee that they are not obliged to report software vulnerabilities to that country's authorities.

The table below maps these requirements across the four assurance levels.[53]

Union assurance level	No obligation to report vulnerabilities to a third country (third-country-controlled providers only)	Software bill of materials (SBOM) and list of dependencies	Safeguards for third-country software (blocking remote features, source code audits, migration plan)	Software components free from third-country control	Safeguards for open-source software (blocking remote features)
Level 4	Not applicable: third-country control excluded	Yes	Replaced by effective control	Yes	Yes
Level 3	Yes	Yes	Yes	No	Yes
Level 2	Yes	Yes	Yes	No	Yes
Level 1	Yes	No	No	No	No

Table 1: Software supply chain criteria across the four Union assurance levels. (Source: Annex II CADA proposal)

[50] Annex III, 6(1) and (2) CADA proposal.

[51] Annex II, 2.1(i), 3.1(i), 4.1(i) CADA proposal.

[52] The introductory text to Annex II says: "'Hardware' within the meaning of Regulation (EU) 2024/2847, Article 3, point (5) is outside of the scope."

[53] The vulnerability reporting guarantee is set out in criterion (g) at level 1 and in criterion (i)(iii) at levels 2 and 3. It does not apply at level 4, where criterion (g) excludes third-country control altogether. The SBOM, third-country software and effective control requirements are set out in criterion (i), and the open-source requirement in criterion (j).

3.3.2. Limitations of assessing software dependencies in isolation

The treatment of hardware is different. Hardware is expressly excluded from the scope of the assurance criteria in Annexes II and III. CADA does address certain aspects of the physical infrastructure used to provide the service, but criterion (b) is concerned only with where that infrastructure and other assets are located. **The framework does not ask questions about who designs or manufactures hardware, including chips, how dependent the provider is on a particular supplier, or whether it could switch to an alternative if access to that hardware were restricted.**

Other EU instruments address aspects of hardware supply-chain security and resilience. The NIS2 Directive requires covered entities to manage cybersecurity risks associated with their supply chains, including risks arising from hardware suppliers.[54] The proposed revision of the Cybersecurity Act addresses security risks in ICT supply chains,[55] while the proposed Chips Act 2.0[56] intends to reduce Europe's strategic dependencies in semiconductor technologies. This may explain why CADA does not seek to regulate hardware dependencies directly. But it does not necessarily explain why hardware dependencies are excluded from the sovereignty assessment altogether.

Notably, the Commission's own Cloud Sovereignty Framework considers hardware supply chains, including the origin of physical components and dependence on non-EU suppliers, demonstrating that hardware dependencies can be a part of a cloud sovereignty assessment.[57]

---

[54] Article 21(2)(d) and (3) NIS2 Directive (n 16).

[55] European Commission, Proposal for a Regulation on the EU Cybersecurity Act (Cybersecurity Act 2.0), <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act> (accessed 25 October 2026).

[56] European Commission, Proposal for a Regulation on a framework of measures for strengthening the Union's semiconductor ecosystem, repealing Regulation (EU) 2023/1781 (Chips Act 2.0), COM(2026) 504 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0504> (accessed 25 October 2026).

[57] Cloud Sovereignty Framework (n 34), SOV-5 (Supply Chain Sovereignty).

Distinction between cloud software and hardware

The distinction between software and hardware dependencies is difficult to maintain in practice, as the two can reinforce each other. Nvidia provides a useful example. Nvidia's GPUs are widely used for AI computing, while CUDA is Nvidia's software platform for using those GPUs. For an AI cloud service that relies on CUDA, this would be the kind of software dependency covered by Annex II. At levels 2 and 3, the provider would need to identify and manage that dependency. At level 4, reliance on CUDA would appear incompatible with the requirement that a third-country entity cannot exercise effective control over software relevant to the provision of the service, since Nvidia controls CUDA's development, maintenance and evolution.

Nvidia's chips, however, are not subject to a dependency test under the sovereignty framework. A provider seeking to offer level 4 AI cloud services would need to consider whether it could use Nvidia GPUs without relying on CUDA or other Nvidia-controlled software. Depending on the workloads and available alternatives, meeting the software sovereignty requirements could constrain the provider's choice of hardware, even though hardware is expressly excluded from the assessment.

3.4. The governance structure: independent auditors but not independent authorities

For levels 2, 3, and 4, whether a cloud computing service fulfils the requirements of the relevant assurance level depends on a decision by the competent national authority,[58] based on the results of an independent third-party audit.[59] This decision is then reviewed by the relevant authorities in other Member States[60] and the Commission can also issue requests to the competent authority for case information during recognition disputes or to trigger compliance investigations.[61]

This procedure raises three questions: first, concerning the evidence available to auditors; second, whether the authorities responsible for recognition and supervision are sufficiently independent; and third, whether the extensive competences of the Commission are justified.

First, Annex III requires auditors to review a wide range of evidence. Much of this evidence will come from the cloud computing service provider itself. The effectiveness of the recognition process therefore depends not only on the independence of the auditors, but also on whether they have sufficient means to identify and verify relevant information beyond what the provider chooses or is able to disclose. Otherwise, auditors may have no way of knowing whether information material to the assessment is missing.

---

[58] Article 17(1), (4) and (5) CADA proposal.

[59] Article 20 CADA proposal.

[60] Article 17(5)(a) and (6)-(9) CADA proposal.

[61] Article 17(13)-(14) and 28(2) CADA proposal.

Second, **the CADA proposal does not require competent authorities in the Member States responsible for recognition and supervision to be institutionally independent.** Member States could designate these functions to, for example, government ministries.

Finally, at EU level, cross-border coordination is necessary to ensure consistent application of the framework and may also help counterbalance the concentration of supervisory responsibility in Member States where major cloud providers are established.[62] Yet the EU-wide consistency mechanism is not entrusted to a board of independent regulatory authorities, as in other regulated sectors. Instead, consistency powers are anchored directly in the Commission, which can issue information and enforcement requests to Member States' competent authorities or override national risk assessments. However, as the executive branch of the Union, the Commission operates as a political actor rather than an independent EU regulatory agency operating at arm's length from industry and politics.

3.5. Key issues

- Recognising third-country control over cloud computing service providers established in the Union would be a step in the right direction compared with the EUCS. However, Union assurance level 2 would still leave room for 'sovereign cloud' arrangements involving US hyperscalers.

- Union assurance level 3 generally excludes third-country control, but the exception for 'associated third countries' leaves open the possibility that the Commission recognises a third country after the CADA is adopted.

- Annex II restricts the use of service-generated data for AI training by third-country actors but does not explicitly extend this prohibition to all customer data, nor does it expressly restrict providers' own use of customer data for AI training within the EU. The broader wording of Annex III creates uncertainty about the intended scope of the safeguard.

- The CADA proposal addresses technological dependencies in software but expressly excludes hardware from the sovereignty assessment, even though software and hardware dependencies are closely interconnected.

- Recognition at Union assurance levels 2 to 4 relies heavily on evidence provided by cloud service providers themselves, raising questions about auditors' ability to independently identify and verify information that providers do not disclose.

- The CADA proposal does not require national competent authorities responsible for recognition and supervision to be institutionally independent, despite the significance of their decisions for the application of the sovereignty framework.

- The EU-wide consistency mechanism is entrusted to the Commission rather than a board of independent regulatory authorities, raising questions about the institutional independence of oversight and the concentration of powers in the Commission.

[62] Article 28 CADA proposal.

4. Demand-side measures

The CADA proposal, once adopted, would introduce EU-wide risk assessments of public sector activities that use cloud computing services, in order to match them to the assurance levels of the cloud computing sovereignty framework. It also prescribes rules on public procurement for contracting authorities in the Member States as well as Union entities. This section will assess the rules on the public sector risk assessments and public procurement from the perspective of promoting European digital sovereignty.

4.1. Risk assessments of public sector activities

One year after CADA's entry into force and then every two years, Member States and Union entities would have to carry out risk assessments that proceed in two sequential steps:

Step 1 (Gateway – prerequisite for entering Step 2):
to identify all public sector activities that 'use or will make use of cloud computing services' and that contribute to 'the preservation of public order'.[63]

Step 2 (Level assignment – substantive risk assessment):
to then determine which Union assurance level – 2, 3 or 4 – is appropriate for the identified public sector activities.[64]

4.1.1. Public sector activities contributing to the preservation of public order

As part of the prerequisite risk assessment, the requirement that a given public sector activity contributes to 'the preservation of public order' would introduce an important legal threshold in the CADA. A public sector activity which does not contribute to 'the preservation of public order' is filtered out at the first step and will not be considered further under the substantive risk assessment criteria of Article 29(2) and will instead be defaulted to cloud computing services recognised at Union assurance level 1 (see Section 4.2.2). Despite this being an important legal threshold, the CADA proposal does not define what contributing to 'the preservation of public order' means. This phrase originates from the general exceptions of the World Trade Organization (WTO) Agreement on Government Procurement,[65] rather than standard EU internal market concepts ('public policy'). **It is never a good idea to leave a central legal concept in a new regulatory framework undefined as this contributes to legal uncertainty and may lead to litigation.**

The public order threshold is also crucial because of how it sequences the risk assessment. The substantive risk assessment under the CADA proposal (see Section 4.1.3) will only take place once a public sector activity has been found to contribute to 'the preservation of public

---

[63] Article 29(1)(a) CADA proposal which further specifies that the public sector activities are 'in sectors falling under Annex I or II of Directive (EU) 2022/2555 and in the areas of national security, internal security, external border management, defence, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal offence'.

[64] Article 29(1)(b) CADA proposal.

[65] See Article III:2(a) Agreement on Government Procurement, as amended on 30 March 2012 <https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.pdf> (accessed 25 October 2026).

order'.[66] One criterion in the second step is for example 'the nature, scope, context and purpose of processing of personal data, as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects'.[67] This risk will not be considered in relation to a public sector activity which has not been found to contribute to 'the preservation of public order' although the risk for individuals' personal data held by a public sector body is equally present here.

The Impact Assessment estimates that the bulk of public sector cloud computing services (circa 70 percent) will not meet this public order threshold and will default to Union assurance level 1.[68] It features a table with an illustrative distribution of criticality of IT systems within a fictitious public sector water company which we have reproduced below (Table 2).[69] This table clearly illustrates that **the CADA proposal's legal threshold of contributing to 'the preservation of public order' effectively restricts which public sector activities will undergo the substantive risk assessment.** This is somewhat illogical, considering that the risk relating to the processing of concerned individuals' personal data is also present with public sector activities that do not directly contribute to 'the preservation of public order'. Why should a public sector entity's payroll, timesheets, holidays and recruitment not undergo the risk assessment foreseen as a second step in the CADA proposal? Arguably, preventing a risk in relation to similar personal data collections in the public sector could also be deemed necessary and proportionate to protect public order.

Non-critical use cases (candidate for level 1)	Critical use case (candidate for levels 2-4)

• **Procurement**
• **Stock management**
• **Inventory**
• **Helpdesk**
• **Billing system**
• **Accounting system**
• **CRM**
• **Workforce management**:
  ○ **Payroll**
  ○ **Timesheets**
  ○ **Training**
  ○ **Holidays**
  ○ **Recruitment**
  ○ …
• **…**
	• Water monitoring system
	• Incident response system
	• Early warning system

Table 2: Illustrative distribution of criticality of IT systems within a fictitious public sector water company. (Source: Impact Assessment, p. 42)

[66] Article 29(1)(a) and (b) CADA proposal.

[67] Article 29(2)(a) CADA proposal.

[68] Impact Assessment (n 37), 41.

[69] Impact Assessment (n 37), 42.

4.1.2. Risk regulation as a technique to comply with international commitments

For cloud computing services used by the public sector, the CADA proposal justifies its use of risk regulation by reference to the EU's international commitments. The Agreement on Government Procurement to which both the EU and the US are parties is invoked to reduce the CADA to information security risk regulation thereby precluding harnessing strategic public procurement as a lever for European digital sovereignty (see Section 2.3). Risk regulation is a technique that has notably evolved to reconcile liberalisation commitments entered into in international trade agreements with restrictions that are deemed necessary to protect public morals, order or safety, among others.

The Agreement on Government Procurement
Out of the 166 members of the WTO, 22 Parties have signed the GPA, among which the US and the EU with regard to its 27 Member States. The EU has committed to the liberalisation of government procurement in the field of computer and related services which covers another Party's cloud computing services without reservations. The GPA mandates non-discrimination whereby each Party commits to accord to suppliers of another Party treatment no less favourable than the treatment the Party accords to its domestic suppliers. The GPA commitments are subject to general exceptions which allow a Party to impose or enforce measures 'necessary to protect public [...] order' provided that such measures do not constitute 'a means of arbitrary or unjustifiable discrimination between Parties [...] or a disguised restriction on international trade'.

The CADA proposal states in that regard:

> *The Union maintains an open and non-discriminatory framework for market access, in accordance with the TFEU and subject to international commitments. Those include commitments under the World Trade Organization (WTO) Agreement on Government Procurement (GPA), as well as bilateral trade agreements. Nevertheless, where necessary and in duly justified circumstances, the Union retains the right, in accordance with Article III:2(a) of the WTO GPA, to adopt or maintain measures necessary to protect public morals, order or safety, allowing for necessary and proportionate restrictions on access to public procurement procedures.*

Risk assessments offer a recognised technique to justify that the restriction is necessary and proportionate. The question thus arises as to what should be considered a risk to public order. The CADA proposal considers that:

> *[...] identifying and addressing risks such as critical dependencies, unauthorised access to Union data, technology leakage, sabotage and espionage by third-country actors is fundamental for preserving Union public order.*[70]

A risk that the CADA proposal does not seek to mitigate head-on is the very high dependence on a small number of third-country cloud providers – a risk that is stressed in

[70] Recital 64 CADA proposal.

the Communication on European Tech Sovereignty, the Explanatory Memorandum to the CADA proposal and the accompanying Impact Assessment.[71] The Impact Assessment moreover articulates other risks that the concentration of cloud computing suppliers in the hands of three large third-country providers[72] has for European public and private customers such as higher prices, lack of alternatives in the event of price hikes, higher egress charges and lock-in effects, and the scale of the impact of outages, citing the CrowdStrike and AWS examples.[73]

Arguably, the current cloud computing market structure in Europe poses in and of itself a dangerous concentration of capacity and power in the hands of a handful of US hyperscalers. There are no economic or political reasons to assume that reducing this one-sided dependency, through an industrial policy that nurtures European cloud service providers to the point where competition is healthy again, would not be necessary to protect public order and the public interest. This objective could also be framed in conformity with the EU commitments entered into with the Agreement on Government Procurement.

If legal advisers in the EU and/or the US argue that the Agreement on Government Procurement requires that the EU lets another party's suppliers by and large usurp the Union's internal market for cloud computing services, then there is something wrong with the commitments the EU entered into. The EU could also revise its commitments and inscribe a cap on market power as a reservation to the Agreement on Government Procurement as the current situation is clearly not in its best interest. Moreover, it is very unlikely that the US, which treats economic security as a subset of national security, would allow covered suppliers from a third country to acquire a more than 70 percent market share of a key domestic market.

4.1.3. The CADA proposal's risk assessment criteria

The risk assessment of public sector activities which have been found to contribute to 'the preservation of public order' then determines at which Union assurance level the contracting authorities can procure cloud computing services. The risk assessment to be carried out by Member States and Union entities incorporates the following aspects:

> *(a) the sensitivity, criticality, and magnitude of the non-personal data processed, including the potential impact on public order and the nature, scope, context and purpose of processing of personal data, as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects;*
>
> *(b) the risk and consequent impact on public order of unlawful access under Union law to such data by a third country or a legal entity established in a third country;*

---

[71] See Explanatory Memorandum to the CADA proposal (n 5), 1: 'three non-EU hyperscalers control over 70% of the European cloud market' and that '[w]hile the EU market for cloud computing services [...] is growing significantly, the market share of EU providers decreased from 29% in 2017 to 15% in 2022'; Communication on European Tech Sovereignty (n 3), fn 17; Impact Assessment (n 37), 12–13.

[72] Impact Assessment (n 37), 12: worldwide, AWS held a market share of 32% in Q2 2024, Microsoft 23% and Google Cloud 12%.

[73] Impact Assessment (n 37), 8 and 12–13.

(c) the risk and consequent impact on public order of possible service disruption.[74]

It is not yet clear how strictly the different criteria will be applied once the CADA risk assessments are carried out. A recital to the CADA proposal signals that:

Most public services would not require the highest levels of assurance. In some specific cases Union assurance levels 3 or 4 may be considered necessary and proportionate in preserving public order. The risk assessment to be performed by Member States and Union entities ensures that the principles of proportionality and subsidiarity are complied with, by assessing the specific cases in which protection of public order requires the highest level of assurance.[75]

The Commission will have decisive influence on the operationalisation of the CADA risk assessments as it has the power to dial down or up how the criteria will be applied:

The Commission shall [...] specify the methodology to be applied, the templates to be used and the elements to be taken into account by the Member States and Union entities for the purpose of carrying out the risk assessments [...]. The methodology shall specify how Member States use the highest level of assurance for the most critical public sectors activities including, but not limited to, defence.[76]

The CADA proposal also tasks the Commission with 'reviewing the results of the risk assessment or assessments of a Member State' and it could effectively overrule a Member State's assessment 'specifying the Union assurance levels needed for the public sector activity.'[77] **Member States would carry out the CADA risk assessments for all public sector activities reliant on cloud computing services at local and municipal, regional and national levels, steered by the Commission, which sets the methodology and has the final say over the results.**

On the one hand, such centralisation could contribute to levelling up and streamlining the assessment of information security risks in public procurement across EU Member States. On the other hand, the centralisation of decision making over the assignment of Union assurance levels to public sector activities across Member States could also limit more ambitious initiatives at local, regional and national levels. It may also have implications for decentralisation and local autonomy across the EU.[78]

---

[74] Article 29(2) CADA proposal.

[75] Recital 52 CADA proposal.

[76] Article 29(3) CADA proposal.

[77] Article 29(5) CADA proposal.

[78] 'Local autonomy is a highly valued feature of good governance.' Andreas Ladner, Nicolas Keuffer and Alexander Bastianen, Self-rule index for local authorities in the EU, Council of Europe and OECD countries, 1990-2020 (European Commission, Publications Office of the European Union 2022), Abstract <https://doi.org/10.2776/803574> (accessed 25 October 2026).

4.1.4. The distribution of public sector activities across Union assurance levels

It is difficult to forecast the outcomes of the risk assessment exercise and the resulting distribution of public sector activities across Union assurance levels. Consider that the risk assessment's purpose is to selectively siphon public sector activities to higher Union assurance levels in order to demonstrate necessity and proportionality under the GPA. The Impact Assessment estimates that:

> *[…] the matching of sovereignty levels to public sector demand follows the following pattern: 70% of use cases would require a sovereignty level 1; 20% for level 2; 9% for level 3; and 1% for level 4. Even though the scheme is novel and does not correspond to existing frameworks, this assessment fits with broad orders of magnitude that can be inferred from existing analyses conducted in several Member States that have introduced risk assessments for their public sector clouds, such as France, Poland or Italy.*[79]

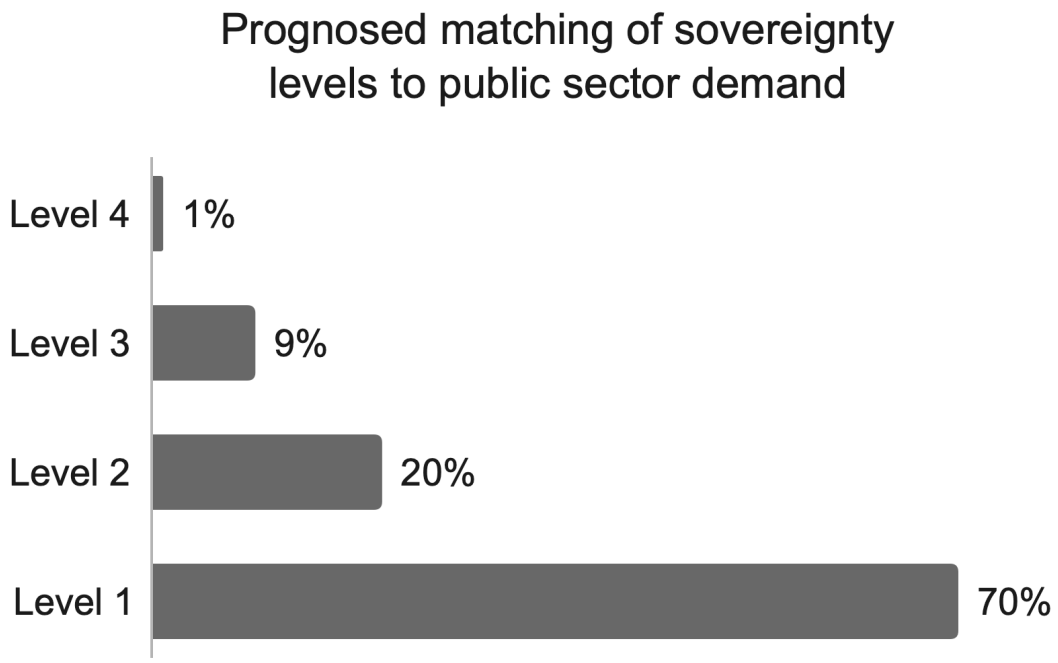


Figure 1: Prognosed matching of sovereignty levels to public sector demand. (Source: Impact Assessment, pp. 41–42.)

As it stands, CADA would have little impact on European digital sovereignty while producing quite an expansive legal framework, procedures and centralisation. Just 10 percent of all public sector activities, those at Union assurance levels 3 and 4, require cloud services free from third-country control (subject to the 'associated third country' exception at level 3), while 90 percent, those at Union assurance levels 1 and 2, can in principle be served by the already dominant US service providers. Would such an outcome really produce progress

[79] Impact Assessment (n 37), 41–42.

towards EU digital sovereignty understood as lessening the EU's dependence on non-European cloud service providers or, rather, lock in the status quo for the time to come?

4.2. Public procurement of cloud computing services

Once public sector activities have been assigned to Union assurance levels, the CADA proposal promulgates requirements for the public procurement of cloud computing services. Once adopted, Article 30 of the CADA proposal would complement and particularise EU public procurement law and be *lex specialis* to the forthcoming Public Procurement Act.[80]

4.2.1. Public procurement of cloud computing services for exclusive use

Article 30(1) of the CADA proposal holds that the provisions of this article apply to contracting authorities and Union entities that procure cloud computing services 'for their exclusive use'. **It is unclear what the term 'for their exclusive use' in the CADA proposal relates to and should be clarified.** According to the authoritative 'NIST Definition of Cloud Computing' only private and community cloud offerings are provisioned for exclusive use, a hybrid cloud can be configured 'for exclusive use' and public cloud offerings are by definition not exclusive (see the box below).[81]

NIST Definition of Cloud Computing
Deployment Models
Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units) [...].
Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns [...].
Public cloud. The cloud infrastructure is provisioned for open use by the general public [...].
Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology [...].

4.2.2. Defaulting public sector activities not contributing to the preservation of public order to Union assurance level 1

Next, Article 30(2) of the CADA proposal is an interesting rule because the proposal does not specify the legal threshold for public sector activities 'contributing to the preservation of public order' (see Section 4.1.1):

> *Union entities and public sector bodies whose public sector activities have not been identified as contributing to the preservation of public order under the risk*

[80] Proposal for a Regulation of the European Parliament and of the Council on public contracts and concessions (Public Procurement Act proposal), COM(2026) 590 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0590> (accessed 25 October 2026).

[81] Peter Mell and Tim Grance, 'NIST Definition of Cloud Computing', NIST Special Publication 800-145 <https://doi.org/10.6028/NIST.SP.800-145> (accessed 25 October 2026).

assessment referred to in Article 29(1) shall use cloud computing services that have been recognised under Article 17 as having a Union assurance level 1.

Once adopted, CADA would harmonise how Member States' public sector bodies – municipalities, regional and national governments – approach public procurement of cloud computing services. They will all be prevented from adopting additional precautions in their public procurement notices for the many functions that, under the CADA, would not be considered to contribute to 'the preservation of public order'. Put differently, **CADA's legal threshold that a public sector activity contributes to 'the preservation of public order' would actually protect the current status quo more than CADA would promote information security or, even further out, digital sovereignty.**

If, for instance, the fictitious public sector water company wants to procure a payroll service that has Union assurance level 3 it would not be allowed to do so once the CADA has entered into force. Under the CADA's harmonised risk assessment, this water company would be required to procure payroll services at Union assurance level 1 because this service did not pass the legal threshold to contribute to 'the preservation of public order'. If it nevertheless publishes a procurement notice with additional safeguards, such as excluding third-country control, an excluded cloud service provider could contest the procedure, and even appeal it in court, as violating the CADA rules (see also Section 4.2.5).

4.2.3. The CADA proposal blocks 'Buy European' at Union assurance levels 1 and 2

Arguably, it would be possible to justify under the Agreement on Government Procurement EU measures which seek to promote market entry, supply chain security and competition by EU cloud computing service providers as necessary to protect public order. At least this is what is happening with regards to the Chips Act 2.0, the proposals for a Public Procurement Act and an Industrial Accelerator Act – all of these initiatives will allow for 'European preference requirements' ensuring that public procurements in critical areas focus on bringing EU added value with economic growth, jobs, and skills located in the Union.[82] The Public Procurement Act proposal has an option to exclude economic operators even from Parties to the GPA when this is justified to avoid 'dependencies [...] that may threaten the security of supply in the Union of the relevant goods or services' and to protect 'economic security interests'.[83]

Once adopted, CADA would become *lex specialis* to the forthcoming Public Procurement Act, thereby foreclosing the option to exclude providers from third countries at Union assurance

[82] See Chips Act 2.0 (n 56); Public Procurement Act proposal (n 80); Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for the acceleration of industrial capacity and decarbonisation in strategic sectors, COM/2026/100 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026PC0100> (accessed 25 October 2026).

[83] Article 72(1)(b) and (c) Public Procurement Act proposal (n 80) which would however require an implementing decision by the Commission.

levels 1 and 2,[84] notably those from the US, which vastly dominate the EU cloud computing market.[85] Considering that the CJEU confirmed that 'the treatment of third-country economic operators in public procurement falls within the common commercial policy, an exclusive competence of the Union',[86] public sector bodies in the Member States cannot adopt or maintain rules that deviate from CADA.

Think for instance of the City of Amsterdam's 'autonomous, unless' cloud strategy which aims to procure 30 percent of its cloud services demand from EU/EEA controlled suppliers by 2030.[87] Unless CADA would become more open and flexible, any ambition to use public procurement strategically in order to reduce public sector dependency on Big Tech may violate EU law. **It would be a missed opportunity not to build 'European preference requirements' into CADA with an option to exclude economic operators even from Parties to the GPA in relation to cloud computing services at Union assurance levels 1 and 2 in order to reduce dependencies, increase supply chain security and economic security more broadly.**

4.2.4. Derogations from assigned Union assurance levels work mostly downwards

The CADA proposal's public procurement rules provide for derogations in three situations, which should be applied on an exceptional basis and where duly justified. The first derogation concerns highly specialised cloud services, which cannot be supplied by cloud computing services already recognised under the cloud computing sovereignty framework.[88] The second allows for derogations when, following a similar procurement process in the previous year, the contracting authority did not receive any suitable tenders.[89] The third derogation applies when applying CADA would require the contracting authority to procure services at disproportionate cost.[90]

In particular the second and third derogation would mostly be invoked to allow procuring cloud computing services at a lower Union assurance level than the one that was assigned to the public sector activity in question. By design, the derogations are of limited practical use and underscore that the CADA proposal amounts to full harmonisation of public sector procurement of cloud computing services in the Union. There are no derogations that allow using higher Union assurance levels than what was assigned.

---

[84] Explanatory Memorandum to the Public Procurement Act proposal (n 80), 2. For possible explanations see Théophane Hartmann, 'EU's tech sovereignty plan risks trade deal, warns US ambassador' (The Rapporteur, 5 May 2026), <https://www.rapporteur.com/news/eus-tech-sovereignty-plan-risks-trade-deal-warns-us-ambassador/> (accessed 25 October 2026).

[85] Impact Assessment (n 37), 12.

[86] Explanatory Memorandum to the Public Procurement Act proposal (n 80), 7 and case-law cited in fn 11.

[87] Gemeente Amsterdam, 'Meerjarenstrategie Digitale Autonomie 2026 - 2035', Versie vastgesteld B&W 20 januari 2026 (in Dutch) <https://openresearch.amsterdam/nl/page/134297/meerjarenstrategie-digitale-autonomie-2026---2035-gemeente-amsterdam> (accessed 25 October 2026).

[88] Article 30(4)(a) CADA proposal.

[89] Article 30(4)(b) CADA proposal.

[90] Article 30(4)(c) CADA proposal.

4.2.5. CADA could supercharge public procurement litigation

In general, public procurement is a heavily litigated field. Harnessing public procurement to reduce dependencies on big tech providers and promoting a European digital stack will be caught between a rock and a hard place. Deviations from the CADA's Union assurance levels can easily be appealed in national courts. The Commission will likely produce a cascade of implementing acts that specify the methodology for the risk assessment, the templates to be used and the elements to be taken into account by the Member States and Union entities. **This detailed regulatory framework could in turn be used by cloud service providers to challenge public sector bodies and contracting authorities in the Member States and Union entities whenever they deviate ever so slightly from the standard track to procure cloud computing services.** Many lawsuits could protract the public procurement of cloud computing services and consequently hold back Member States' effective adoption of a resilient cloud computing public sector stack.

The water company example in a nutshell

The water company wants to purchase cloud services for managing its payroll.

Step 1: Which assurance level does the activity need? The public order test decides whether an activity qualifies for Union assurance level 2, 3 or 4. A water company's payroll service does not contribute to 'the preservation of public order', so it defaults to Union assurance level 1.

Step 2: Can the water company include requirements from level 2, 3 or 4 in the tender? No. Once an activity has been found not to contribute to public order, nothing justifies a higher-level requirement.

Step 3: Could a provider offering those higher assurance levels bid? Yes. Higher levels include the criteria of the lower ones so a level 2 or 3 service also meets level 1, and the bidder can compete.

Step 4: Could the water company give a higher weight to a provider offering higher assurance levels? That depends on how Article 30(2) is read. Public sector bodies 'shall use' services 'recognised … as having a Union assurance level 1.' If it is read as 'level 1 only', the contracting authority cannot reward a provider for offering higher assurance levels, as this is not part of the procurement notice and would disadvantage other bidders.

Step 5: Could the water company use a derogation? Hardly. The derogations cover the cases where no suitable recognised service exists, no suitable tenders were received in the previous year, or costs would be disproportionate. They would mostly be used to procure below the assigned level, not above it.

Step 6: What if it publishes a tender with additional safeguards anyway, such as excluding third-country control? A provider could challenge the procedure in national courts as violating the CADA.

Optional: Could the water company inscribe open source as a quality requirement in the public tender next to the Union assurance level 1? Yes, that would be an option but all providers at Union assurance level 1 who offer a payroll SaaS that is open source must be considered, including companies from third countries.

4.3. Additional measures to enhance resilience and limit dependency

The CADA proposal puts forward a few measures that could help reduce provider lock-in and enhance sovereignty. However, the scope and reach of these measures are limited or optional.

Firstly, Member States and Union entities must in the course of making their risk assessments consider 'whether a multi-vendor or multi-cloud strategy is appropriate as part of their procurement of cloud computing services'.[91] They are not obliged to adopt such a strategy, which would avoid single points of failure across public sector cloud computing usage.[92] Emphasising multi-vendor or multi-cloud strategies would indeed help enhance resilience and limit dependency on a single cloud computing service provider and should be promoted as a best practice demand-side measure.

Secondly, the CADA proposal introduces 'Union added value' as a non-price award criterion in public procurement procedures. However, this criterion applies only to 'innovative' cloud computing services and AI systems.[93] In addition, the criterion is explicitly designed as 'ancillary and not decisive'[94] since a maximum weighting (15 out of 120 points) would ensure that the other criteria (price and quality) remain primary.[95] The CADA proposal would prevent contracting authorities from using 'Union added value' as a decisive factor. Furthermore, the CADA proposal requires Member States to 'pursue as objective that at least 25% of their procurement for cloud computing services and AI systems be awarded to innovative SMEs'.[96] This is a target, not an obligation, which is limited to SMEs offering 'innovative' cloud computing services and AI systems.

Thirdly, Union entities and public sector bodies should be encouraged 'to use and facilitate the reuse of open standards and components released under an open source licence when building their cloud and AI ecosystem or stack'.[97] Again, this is a requirement to encourage, not to prioritise, open source. Yet, open source-based cloud services are key for increasing resilience and reducing the current overdependence on proprietary services from three US hyperscalers.

Taken together, the multi-vendor/-cloud strategy, Union added value and open standards may steer public procurement by public sector bodies and Union entities in the direction of improved digital sovereignty and better resilience. Because none of them is binding in its outcome, they are less likely to contribute to digital sovereignty in public sector cloud use.

---

[91] Article 29(9) CADA proposal.

[92] See the Impact Assessment to the CADA proposal (n 37), 13.

[93] Article 32 CADA proposal.

[94] Article 32(2) CADA proposal.

[95] Recital 67 CADA proposal.

[96] Article 33(4) CADA proposal.

[97] Article 41 CADA proposal.

4.4. Key issues

- The meaning of a public sector activity contributing to 'the preservation of public order' (Article 29(1)(a)) is not defined. As this is an important legal threshold in the CADA for the risk assessments of public sector activities it should also be defined in the legislation.

- The CADA proposal's legal threshold of contributing to 'the preservation of public order' effectively excludes public sector activities at Union assurance level 1 (circa 70 percent) from being assessed following the risk assessment criteria in Article 29(2).

- Member States would carry out the CADA risk assessments for all public sector activities reliant on cloud computing services at local and municipal, regional and national levels, steered by the Commission, which sets the methodology and has the final say over the results, thereby reconfiguring local autonomy and decentralisation across the EU.

- As it stands, CADA would have little impact on European digital sovereignty while producing quite an expansive legal framework, procedures and centralisation. The risk that the CADA proposal does not mitigate head-on is the very high dependence on three US hyperscalers which control more than 70 percent of Europe's cloud market.

- It would be a missed opportunity not to build 'European preference requirements' into CADA in relation to cloud computing services at Union assurance levels 1 and 2 to reduce dependencies, increase supply chain security and economic security more broadly.

- This detailed regulatory framework could be used by cloud service providers to challenge public sector bodies and contracting authorities in the Member States and Union entities whenever they deviate ever so slightly from the Union assurance levels.

- Three additional measures to enhance resilience and limit dependency – a multi-vendor/-cloud strategy, Union added value and open standards – may together steer public procurement by Member States' public sector bodies and Union entities towards improved sovereignty and better resilience; yet the scope and reach of these measures are limited or optional.

- The CADA proposal is not ambitious enough in 'leveraging public procurement to support the deployment and scaling of open and interoperable digital solutions' as called for by the European Parliament in its 2026 resolution on European technological sovereignty.

5. Conclusions and recommendations

In this report, we analysed Title IV of the CADA proposal, which sets the rules for supplying cloud computing services to public sector bodies through Union assurance levels and for public sector demand through risk assessments and public procurement rules. Our analysis revealed that, in its current form, CADA is more likely to reinforce the public sector's reliance on a limited number of non-EU providers than to mitigate it.

Based on this analysis, we make the following recommendations.

Remove contributing to the 'preservation of public order' as the threshold for higher sovereignty levels or, at a minimum, define it broadly.	**Articles 29(1)(a), 29(2), 30(2) CADA proposal**

Public order should not be the legal threshold for pursuing greater cloud sovereignty through public procurement. If the notion is read narrowly, about 70 percent of public sector activities are never assessed following the actual risk assessment criteria, and Union assurance level 1 becomes a ceiling for them. The notion is also undefined. That leaves legal uncertainty, and it gives providers grounds to challenge any contracting authority that asks for more. If the notion is kept, it should be defined in the operative text to cover critical dependencies, economic security risks and lock-in, as recitals 49, 50 and 64 already do, and the sectoral limitation in Article 29(1)(a) should be removed. Internal processes and functions of public sector bodies should also be considered as contributing to the preservation of public order. If this is not accommodated, Title IV should be renamed as an 'information security risk framework', making clear that its procurement rules are *not* designed to diversify the cloud market or reduce reliance on a small number of non-EU providers.

Allow higher assurance levels beyond public order activities	Article 30(2) CADA proposal

Clarify Article 30(2) so that public sector bodies whose activities have not been identified as contributing to the preservation of public order must use at least Union assurance level 1, but remain free to require a higher level, or individual criteria from higher levels, in their tenders. This could be done by replacing 'as having a Union assurance level 1' with 'as having at least Union assurance level 1'. The Explanatory Memorandum already describes level 1 as a minimum requirement, suggesting that the framework is intended to establish a baseline rather than a ceiling on cloud sovereignty. Clarify in a recital that public sector bodies may seek higher Union assurance levels when procuring cloud computing services.

Regarding sovereignty assurance levels	Annex II, CADA proposal

Amend criterion (f) in points 2.1, 3.1 and 4.1 of Annex II to prohibit the use of customer data processed, stored or generated through the audited service for training or fine-tuning any AI system without the explicit authorisation of the public sector body, rather than limiting

the restriction to data generated through the use of the service and to AI systems operated by third-country entities. This would align Annex II with Annex III, which already refers to data being processed solely for the delivery of the audited service.

Extend the CADA's assessment of technological dependencies beyond software to include critical hardware components and supply chains, building on the approach adopted in the Commission's Cloud Sovereignty Framework (SOV-5 Supply Chain Sovereignty). Delete the hardware exclusion clause in the introductory paragraph of Annex II. The proposal already recognises the relevance of hardware in the Union added value criteria (Article 32(3)(a) and (d)). Requirements could be graduated, starting with transparency about the origin of critical hardware at lower levels.

Foresee that independent auditors and independent national supervisory authorities can validate the evidence provided by the cloud computing service provider by means of technical audits. Add the necessary powers to the CADA proposal to access source code for auditing purposes, analyse data flows and request necessary data from the provider subject to professional secrecy obligations.

Make the designation of associated third countries under Article 18 subject to a public consultation, and require the Commission to publish its assessment of how the third country meets each of the cumulative criteria in Article 18(1). Given that a designation could open Union assurance level 3 to providers controlled from a third country, the decision should be open to public scrutiny.

Regarding additional measures:	
Union added value	Articles 32(1), 32(2)(d), 32(3), recital 67 CADA proposal
Multi-vendor/-cloud strategy	Article 29(9) CADA proposal
Open standards	Article 41 CADA proposal

Extend the application of the Union added value criterion beyond just innovative cloud computing services and AI systems to public procurement of cloud services more generally, by deleting 'innovative' in Article 32(1). Recital 67 already refers to public procurement procedures for cloud computing services and AI systems without this limitation. Add open source and interoperability to the criteria in Article 32(3): the use of software released under an open source licence, of open standards and open specifications, and the ease of switching providers and porting data. Allow this criterion to carry greater weight in contract awards, rather than remaining merely ancillary and non-decisive, to help diversify public sector demand and reduce lock-in. This means deleting point (d) of Article 32(2) and the 15/120 point restriction in recital 67, and allowing contracting authorities to assign a weighting of up to 30% to these criteria. Unlike criteria based on origin, open source and interoperability criteria do not discriminate between suppliers by nationality, which makes them easier to defend under the GPA.

Make multi-vendor or multi-cloud strategies the default rather than an option to consider. Amend Article 29(9) so that Member States and Union entities that do not adopt such a

strategy must explain why. Introduce monitoring and reporting about adopting multi-vendor or multi-cloud strategies and set progressive targets for public sector bodies in the Member States and Union entities.

Turn the duty to encourage open source in Article 41 into an 'open source first' rule. Union entities and public sector bodies should use open standards and components released under an open source licence when building their cloud and AI stack, unless they justify why a proprietary solution is needed, taking into account functionalities, security and total cost.

Regarding the CADA proposal's institutional governance and process	Articles 17(10), 25(3), 28, 29(5) of the CADA proposal

Amend Article 25(3) to require that competent authorities are set up and act with complete independence, free from political direction and commercial influence.

Entrust EU-level coordination and consistency functions to an independent board composed of national competent authorities, instead of concentrating these powers in the Commission. Transfer the binding decision on disputes over recognition under Article 17(10) from the Commission to this board. The deadline in Article 28(4) for the competent authority of establishment to act on a request should be shortened from two months to one month, after which the requesting authority should be able to refer the matter to the board.

Limit the Commission's power under Article 29(5) so that it can only raise the Union assurance level a Member State has identified, not lower it.

Taken together, these changes would allow public authorities to use procurement not only to manage their reliance on a small number of non-EU providers, but to reduce it. As it stands now, the CADA proposal is not ambitious enough in 'leveraging public procurement to support the deployment and scaling of open and interoperable digital solutions' as called for by the European Parliament in its 2026 resolution on European technological sovereignty.

Annex

Level	(a) Establishment	(b) Infrastructure & assets	(c) Customer data localisation	(d) Personnel	(e) Cybersecurity	(f) Data generated through use / AI	(g) Third-country control	(h) Technical and operational support	(i) Software dependencies	(j) Open-source software	(k) Third-country operations
Level 4	Same as level 2	Same as level 2	Sensitive customer data identified through risk assessment must remain in EU	Same as level 3	'High' cybersecurity assurance under an applicable EU certification scheme or equivalent	Same as level 2	Prohibited; no associated-country exception	Same as level 3	Effective control over relevant software required	Same as level 2	Same as level 2
Level 3	Same as level 2	Same as level 2	Same as level 1	Relevant personnel must be EU citizens; security clearance where appropriate	Same as level 2	Same as level 2	Generally prohibited; associated-third-country exception	As level 2 plus support personnel must be EU residents and support providers free from third-country control	Same as level 2	Same as level 2	Same as level 2
Level 2	Provider + relevant subcontractors established in EU	Located in the EU	Same as level 1	EU citizenship/ screening where required	At least 'substantial' cybersecurity assurance under an applicable EU certification scheme or equivalent	No transfer outside EU or AI training/fine-tuning by third-country actors	Permitted, but safeguards must prevent third-country control from affecting service delivery, customer data or continuity	Support must be performed exclusively in EU	Identify and manage software dependencies; safeguards against third-country interference plus migration plan	Safeguards against remote tampering or interference	Effective separation between EU parent and third-country subsidiaries
Level 1	Provider established in EU	Located in the EU, unless the public sector customer requires otherwise.	Customer data, including metadata and telemetry, must remain in the EU, unless the public sector customer requires otherwise.	No citizenship requirement	State-of-the-art cybersecurity measures	No equivalent requirement	Permitted	Outside-EU support possible with safeguards	No equivalent requirement	No equivalent requirement	No equivalent requirement

Table 3: CADA cloud sovereignty criteria across the four Union assurance levels.

About this report

Dr. Zuzanna Warso is Director of Research at Open Future. Her current research and publications focus on EU AI industrial policy, including questions related to public and private investment, transparency, infrastructure governance, and the political economy of AI development.

Dr. Kristina Irion is an Associate Professor at the Institute for Information Law (IViR) at the University of Amsterdam. In her research, Dr. Irion focuses on EU digital and data law in relation to the governance of transnational digital technologies and data flows. She has published on sovereignty and jurisdiction in relation to transnational cloud computing and international (digital) trade law.

Open Future is a European think tank that develops new approaches to an open internet, maximising the societal benefits of shared data, knowledge, and culture. The organisation creates strategies for Digital Commons—democratically governed, collectively managed resources that provide an alternative to traditional ownership models. Open Future focuses on reimagining openness to foster a more balanced digital future that serves the public interest.

The Institute for Information Law (IViR) at the University of Amsterdam is one of the largest research centres in the field of information law in the world. The Institute's mission is to further the development of information law within a legal framework that accommodates the needs and interests of the information society, its citizens and its industries in a just and balanced way, while respecting fundamental rights and democratic freedoms. IViR research aims at producing scholarly output that lives up to rigorous academic standards, while feeding into societal discussions and policy debates on information law-related issues.

This report is published under the terms of the Creative Commons Attribution License.

Suggested citation:

Zuzanna Warso and Kristina Irion, 'The Cloud and AI Development Act Proposal: Extensive Regulation for Limited Sovereignty Gains?' (Open Future and Institute for Information Law (IViR), November 2026). https://openfuture.eu/publication/the-cloud-and-ai-development-act-proposal/