University of Amsterdam
Institute for Information Law

IViR Position Paper

The EU's Proposal for a Cloud and AI Development Act: Not the Industrial Policy the EU Needs

November 2026

IViR Position Paper

The EU's Proposal for a Cloud and AI Development Act: Not the Industrial Policy the EU Needs

The Institute for Information Law (IViR), Amsterdam. 5 November 2026

Created by

Dr Plixavra Vogiatzoglou, corresponding author: p.a.vogiatzoglou@uva.nl
Dr Kristina Irion
Anushka Mittal
Dr Laurens Naudts
Dr Charis Papaevangelou

The views expressed in this report are those of the authors and do not necessarily reflect those of the organisations. Responsibility for any remaining errors or omissions rests solely with the authors.

Citation

P. Vogiatzoglou, K. Irion, A. Mittal, L. Naudts and Ch. Papaevangelou, IViR Position Paper 'The EU's Proposal for a Cloud and AI Development Act: Not the Industrial Policy the EU Needs', Amsterdam, Institute for Information Law (5 November 2026), <https://www.ivir.nl/publicaties/download/CADA.pdf>.

This work is licensed under Creative Commons Attribution-NoDerivatives 4.0 International. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/4.0/

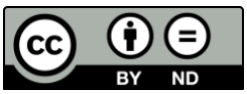


Table of contents

A. Cloud and AI Leadership Initiatives 4
B. Data centre capacities 6
C. Cloud computing sovereignty framework & demand-side measures 7
D. Union assurance levels under Annex II: 10
E. Cloud federation & open source 12

In 2025, the European Commission decided to address European Union (EU)'s stark dependence "on a limited pool of third-country providers", where "three non-EU hyperscalers control over 70% of the European cloud market."[1] The Commission's proposal for the Cloud and AI Development Act (CADA) states that it seeks "to address the limited and geographically concentrated availability of computing capacity in the EU and the risks associated with dependence on cloud and AI supplied by non-European providers."[2] To ensure this increase in EU-based compute and AI uptake, the CADA proposal would set more attractive investment conditions by lowering administrative red tape and simplifying permit standards for a massive build-out of data centre capacity. At the same time, the CADA proposal would introduce a risk-based framework for public sector uses of cloud computing which would reduce reliance on non-European cloud computing services for public sector activities that contribute to the public order.[3] The proposal aims to realise these ambitions by A) promoting cloud and AI leadership strategies, B) expanding data centre capacities, C) establishing a cloud sovereignty framework with demand-side measures and D) Union assurance levels, and finally E) supporting open source. This position paper examines this five-pronged approach to identify current gaps and ways to address them, as CADA is in the legislative proposal phase.

A. Cloud and AI Leadership Initiatives

- **An inflation of AI's capabilities:** recital (1) claims that "by enabling faster innovation, greater efficiency and smarter decision-making, AI contributes to substantial economic, environmental and societal gains and is a fundamental driver of competitiveness." Where AI is designed to produce those outcomes, it may indeed have these benefits. Still, the proposal chooses to remain silent about the societal (including fundamental rights risks) and environmental costs associated with the deployment of AI-driven technologies and (material) infrastructures necessary to facilitate their uptake. The proposal could more explicitly recognise how the acceleration of cloud and AI initiatives may negatively impact fundamental rights, the labour market, local communities and the environment. In particular, the proposal could acknowledge how normative choices made at the infrastructural level (e.g., how to allocate compute or storage capacity) affect later stages of the AI-value chain, including the roll-out of technologies that facilitate (mass) data collection, data-driven manipulation, and surveillance.[4]

- **The leadership initiatives' general objectives impose a self-fulfilling logic:** The leadership initiatives pursue the general objective of promoting research and innovation activities and

[1] 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 – CADA proposal), COM/2026/502 final, p 1.
[2] Ibid, p 2.
[3] Ibid, p. 3-4.
[4] See, for example, Data Center Working Group, 'Data Center Site Fight Guide: A Shared Resource for Stopping Data Centers' <https://docs.google.com/document/d/143tA8XVh7de9MD2GBiKQ3BcMFqeonlqx7EsoIy_olfQ/edit?tab=t.9tvjsz4902n6>; Harry Davies and Yuval Abraham, '"A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians' *The Guardian* (6 August 2025) <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud> accessed 2 November 2026.

achieving large-scale capacity throughout the Union's digital ecosystems. According to Article 3(1)b, this objective can be realised by "reinforcing the Union's data centre and cloud capacity to meet the growing demands driven by AI". Simultaneously, Article 3(1)(c) claims the CADA's overarching objective entails "stimulating [of] the Union's demand and promoting the deployment and uptake of cloud and AI technologies across the public sector and the private sector." In other words, the CADA proposal addresses a demand that the Union itself encourages the public and private sector to pursue. While explicitly not intended as a "harmonising" effort, in so doing, the CADA proposal encourages Member States to pursue a "The More AI The Better" approach at all societal costs.

- **Operational objectives lack democratic desiderata:** The proposal could have incorporated democratic governance standards when specifying the leadership initiatives' operational objectives.[5] Likewise, the operational objectives would benefit from the input of affected persons.[6] While European Digital Innovation Hubs,[7] Experience and Acceleration Centres for AI,[8] and the AI Board could play a facilitating role in bringing together diverse stakeholders, the CADA proposal, as it stands, is silent on local and democratic engagement, with participation by civil society and affected persons largely omitted. Though Member States are not precluded from attaching democratic criteria to these objectives, such criteria should not be optional, which the proposal risks doing. One of the CADA's sole concessions to the public concerns Article 12(2)(e), which lists as a potential role of the single information points designated within data centre projects in acceleration zones to "[inform] the public, with the aim of increasing public acceptance of the data centre project." This phrasing, however, positions the public not as an affected community or participatory partner, but rather as a stakeholder that must be informed and, above all, convinced about the virtues of the envisaged projects. Rather than merely consult societal stakeholders, a more integrated approach toward democratic multi-stakeholder or commons-inspired infrastructure governance could help ensure that the CADA contributes to the development of a truly public stack.[9]

- **No room for local, smaller-scale community-led initiatives?** By focusing on large-scale data infrastructures, the Leadership Initiatives risk precluding the emergence of small-scale, community-led alternatives. It nonetheless remains important that these alternative ecosystems can be researched, and doing so would be in line with the European Declaration on Digital

[5] Article 4 CADA proposal.

[6] See for example, Operational Objective 8 which seeks to "promote the broad adoption of AI by private and public sector organisations, including SMEs and SMCs, through the network of Experience and Acceleration Centres for AI ('Centres for AI')." Likewise, Article 7(2)c encourages the national strategy to take "measures to support the deployment of data centre capacity, with a particular focus on high-value data centres delivering significant economic and societal benefits while adhering to high environmental and energy-efficiency standards."

[7] Recital (25) CADA proposal, Article 16 Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166, 11.5.2021, pp. 1–34.

[8] Article 5 CADA proposal.

[9] See for example Cecilia Rikap and others, 'Reclaiming Digital Sovereignty: A Roadmap to Build a Digital Stack for People and the Planet' (A collective proposal by the Democratic and Ecological Digital Sovereignty Coalition 2024) <https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/reclaiming-digital-sovereignty.pdf> accessed 2 November 2026; Francesca Bria, Paul Timmers and Fausto Gernone, 'EuroStack – A European Alternative for Digital Sovereignty' (Bertelsmann Stiftung 2025) doi/10.11586/2025006.

Rights and Principles. The proposal mentions that Leadership Initiatives may be supported through Union Initiatives, including Horizon Europe and the Digital Europe Programme, but it remains to be seen whether these actions are truly open to exploring public interest-oriented digital infrastructures (e.g., community data centres, locally run shared clouds, open-source not-for-profit cloud stacks, etc.) that, too, can reduce dependencies and increase digital sovereignty.

B. Data centre capacities

- **Acceleration without sustainability?** The CADA proposal's Title III 'Data Centre Capacities' proposes the expedition and support of data centre construction through two ways: a) the designation of "acceleration zones" by Member States within their countries,[10] and the designation of "strategic projects" by a separate Commission process.[11] Regarding the former, projects within these zones would receive administrative assistance and accelerated permitting and would be further supported by legal obligations on the side of the public authorities.[12] Member States would thus play an active role in facilitating the industry's growth. The latter allows the Commission, following an open call for expressions of interest, to designate projects meeting at least two of five criteria as strategic, with possible support coming from the Union's relevant funding programmes.[13] Sustainability is only one of these criteria,[14] so a project can be designated without it contributing to the EU's overarching goal for a green transition.

- **Weak connection between expanding computing capacity and sustainability:** Member States are instructed to use the key performance indicators (KPIs) of Delegated Regulation (EU) 2024/1364[15] to set sustainability requirements for data centres in acceleration zones.[16] But the KPIs invoked are limited to (a)-(n) of the Delegated Regulation's Annex II, excluding (o)-(r) on total renewable energy consumption and its sources, potentially hindering transparency about a crucial vector like measuring how much of the electricity consumed by a data centre is generated via renewable sources and through which channels it is sourced. Relatedly, the Commission is tasked only with tracking available computing capacity, demand, and the resulting "capacity gap",[17] leaving Member States to monitor the environmental impacts of acceleration zones.[18] Notably, the proposal does not introduce a methodology for how this gap will be calculated or how Member States should measure those impacts. This situation could therefore lead to a further fragmented and unclear overview of the actual resources consumed by data centres, risking exacerbating the "race to the bottom" that the CADA proposal seeks to avoid.[19] Indeed, the current reporting experience with the Energy Efficiency Directive

[10] Article 10 CADA Proposal.
[11] Article 14 CADA proposal.
[12] Articles 12-13 CADA proposal.
[13] Recital (43) CADA proposal.
[14] Article 14(1)(b) CADA proposal.
[15] Commission Delegated Regulation (EU) 2024/1364 of 14 March 2024 on the first phase of the establishment of a common Union rating scheme for data centres, OJ L, 2024/1364, 17.5.2024.
[16] Article 11(1) CADA proposal.
[17] Article 15 CADA proposal.
[18] Article 10(2)(a) CADA proposal.
[19] CADA proposal, p. 7.

obligations[20] offers little reassurance vis-à-vis transparency obligations.[21] It is also worth highlighting that virtually no attention seems to be paid to the social impacts of the envisioned data centre build-out.

- **Watering down Environmental Impact Assessments:** Crucially, under Article 13(1) CADA proposal, projects within acceleration zones would receive privileged treatment as strategic projects according to the proposed Regulation for Speeding-up Environmental Assessments.[22] For instance, Recital 14 leaves the door open to encouraging less stringent Environmental Impact Assessments (EIAs), allowing Member States to determine whether they are needed. EIAs are far from a perfect instrument, but they can provide information for public scrutiny, including data centre developers' rationales for the choices made, making data centre projects more publicly visible and, potentially, democratically contestable. Worryingly, these advantages would replicate and scale up selected national frameworks that already follow that principle. In Greece, for example, data centres between 2-20 MWs fall under standard environmental pledges rather than full EIAs.[23]

- Fundamentally, governing data centre development, especially at large scale, concerns how societies allocate finite resources, from water and (preferably renewable) energy to land and electricity grid capacity. Even when these facilities meet their energy needs through their own renewable generation, they still occupy land and consume scarce resources that could serve other needs, including decarbonising other sectors and activities. Deciding which needs take priority is therefore a question of distribution: who benefits from these resources and whose needs are left behind? The CADA proposal, as it stands, seeks to (re)orient state planning and allocation of public and natural resources to increasing data centre build-outs, thereby prioritising the cloud computing sector over other sectors. Yet the proposal does not demonstrate convincingly why these facilities should take priority over competing societal needs; rather, their expansion appears to be a means in and of itself. Finally, the CADA proposal seems to assume that data centre expansion will lead to sovereign compute but does not provide a concrete framework to that end, nor does it expressly link Title III with Title IV 'Autonomy'.

C. Cloud computing sovereignty framework & demand-side measures

- **Limited scope and effect**: The Union assurance levels apply to cloud computing services provided to public sector bodies in the Member States and EU entities.[24] The CADA proposal clarifies how these assurance levels are intended to be applied to public sector activities in the following chapter ('Demand-side measures'). According to Article 29, public sector activities

[20] Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955, OJ L 231, 20.9.2023, pp. 1–111.
[21] See, for instance, a recent legal filing by Lighthouse Reports to the Aarhus Convention Compliance Committee regarding transparency around data centres' energy consumption <https://www.lighthousereports.com/wp-content/uploads/2026/09/2026-09-25-Lighthouse-Reports-Aarhus-Compliance-Committee-Communication.pdf> accessed 2 November 2026.
[22] Proposal for a Regulation of the European Parliament and of the Council on speeding-up environmental assessments, COM(2025) 984 final, 2025/0391 (COD).
[23] Ministerial Decision ΥΠΕΝ/ΔΙΠΑ/82255/5190/2025.
[24] Article 16 CADA proposal.

contributing to the "preservation of public order" (see also below) should be subject to Union assurance levels 2, 3 or 4. However, the vast majority of public sector bodies, that is, those not performing tasks of public order relevance, but all other public administration and public service bodies, such as education, media and cultural bodies, and public sector activities, such as payroll systems or workforce management, are subject to the least strict Union assurance level 1. In this way, the CADA proposal would prevent most public sector activities from requiring higher protection under Union assurance levels 2-4. According to the Commission's own assessment: "70% of use cases would require a sovereignty level 1; 20% for level 2; 9% for level 3; and 1% for level 4."[25]

- **Unclear criteria:** One year following the CADA's entry into force and then every two years, Member States and Union entities shall carry out risk assessments to identify public sector activities "that contribute to the preservation of public order" including in the areas of national and internal security, border management, justice or law enforcement.[26] The proposal does not define what contributing to "the preservation of public order" means. The phrase uses World Trade Organisation (WTO) Agreement on Government Procurement (GPA) trade exception terminology[27] rather than EU law concepts (e.g., "public interest"). 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 obscures how it will be used.

- **Role of the Commission:** According to the CADA proposal, when conducting such a risk assessment, Member States, public sector bodies, and EU entities must take into account three risk criteria, including the sensitivity of data processed, the risk of unlawful access and the risk of disruption of services. Yet it further foresees that the Commission will adopt "a methodology to be applied, the templates to be used and the elements to be taken into account" for the CADA risk assessments.[28] In other words, CADA envisages that the Commission will orchestrate a pan-European risk assessment for all public sector activities reliant on cloud computing services at local and municipal, regional and national levels as well as EU entities.

- **Beyond the Union assurance levels?** Importantly, by harmonising how Member States' public sector bodies - municipalities, regions, national governments and providers of services of general interest-approach public procurement of cloud computing services, the CADA proposal would preclude them from adopting additional precautions in their public procurement notices for many of their functionalities that would not be considered to contribute to "the preservation of public order." Under Article 30(4), all public sector bodies may derogate from the assigned Union assurance levels where at least one of the following circumstances applies: (i) the tender subject matter cannot be supplied, and there are no adequate or reasonable alternative services;

---

[25] 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), SWD/2026/502 final, Part 1, p. 41.
[26] Article 29(1) CADA proposal.
[27] Recital (64) CADA proposal with reference to Article III:2(a) Agreement on Government Procurement 2012, <https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.pdf > accessed 2 November 2026.
[28] Article 29(3) CADA proposal.

(ii) there were no suitable tenders or participants; and (iii) the cost would be disproportionate. The derogations would allow public authorities to use a lower Union assurance level than the one that was originally assigned. It provides downward, not upward flexibility.

- **Risk of litigation against public sector bodies**: Deviations from the CADA proposal's Union assurance levels can easily be used to appeal public procurement procedures in national courts. This regulatory framework could be used by cloud services providers to challenge contracting authorities in the Member States and Union entities whenever they deviate even 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.

- **Private entities:** Private entities, in principle, fall outside the scope of the CADA proposal's provisions. From the demand side, if a private body is tasked with preserving public order, such as banks and other critical infrastructure operators, they may conduct similar risk assessments.[29] From the supply side, there is no concrete guidance or obligation for European cloud service providers to reach the threshold of the Union assurance levels, especially given the low percentage of activities requiring more than level 1.

- **Enforcement:** For Union assurance level 1, cloud computing service providers may perform a self-assessment of conformity, whereas for Union assurance levels 2, 3, and 4, providers must undergo an independent third-party audit.[30] This pattern of entrusting the private (tech) sector with setting, and thus interpreting, standards and enforcing EU legislation has already drawn criticism in relation to other EU digital regulation.[31] But the independent auditors, too, would rely on the evidence provided by the cloud service providers for being accredited at levels 2, 3, and 4. It raises questions about accountability for legal compliance with Union assurance levels and, more broadly, the robustness of a scheme that cannot be independently verified. Similarly, national competent authorities should be designated to enforce the CADA "in an impartial, transparent and timely" but not explicitly independent manner.[32]

- **Measures that could help reduce provider lock-in and enhance sovereignty:** Firstly, Member States and Union entities can, in the course of making their risk assessments, explore "whether a multi-vendor or multi-cloud strategy is appropriate as part of their procurement of cloud computing services."[33] Secondly, the CADA proposal introduces "Union added value" as an award criteria in connection with "public procurement procedures for "innovative cloud computing services and AI systems."[34] However, those are explicitly designed as "ancillary and

[29] Article 31(1) CADA Proposal.
[30] Articles 19 and 20 CADA Proposal respectively.
[31] Nathalie A Smuha and Karen Yeung, 'The European Union's AI Act: Beyond Motherhood and Apple Pie?' in Nathalie A Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press 2025) <https://doi.org/10.1017/9781009367783.015> p. 252-257.
[32] Article 25 CADA proposal.
[33] Article 29(9) CADA proposal.
[34] Article 32 CADA proposal.

not decisive."[35] 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 license when building their cloud and AI ecosystem or stack."[36] The optional and limited scope of these provisions would make it unlikely to yield a sizable effect and they should be made more ambitious (open source first, Union added value not limited to "innovative" cloud computing services and AI systems, multi-vendor or multi-cloud strategy by default).

D. Union assurance levels under Annex II:

- **Criteria largely not excluding Big Tech cloud services providers:**
  - The criteria around which the four levels are structured may be roughly summarised as comprising: location of provider's and subcontractor's establishment; location of infrastructure, assets and data; citizenship of working personnel; cybersecurity standards; technological and operational support; software supply chain; contractual relationship to subcontractors and subsidiaries; being subject to control by a third country. The strictness of the criteria varies by level. The decisive criterion of control should be understood in line with the European Defence Fund as "the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities."[37]
  - For Union assurance level 1, it suffices to ensure data localisation in Europe and implement organisational and technical measures for data protection and cybersecurity to comply with the General Data Protection Regulation[38] and the NIS 2 Directive[39].
  - For Union assurance levels 2-3, most of the requirements, such as personnel's obligation to hold EU citizenship (and thus formally delimit any link or control by a third country), the availability of open-source software, and the implementation of sufficient controls against software tampering, could be met by Big Tech cloud products and commitments (e.g., see Microsoft digital commitments[40]). A cloud service provider may be considered for Union assurance level 3 when it is subject to an adequacy decision adopted under the GDPR, such as, for example, the currently valid EU-US Data Privacy Framework.[41] However, in that case, the cloud service provider must also demonstrate that no measures in the third country enable access to data or disruption of services, which brings back the question of how convincing Big Tech commitments are.

---

[35] Article 32(2) CADA proposal.
[36] Article 41(1) CADA proposal.
[37] Article 2(21) CADA proposal with reference to Article 2(6) Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092, OJ L 170, 12.5.2021, pp. 149–177.
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR) OJ L 119, 4.5.2016, pp. 1–88.
[39] 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 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152.
[40] Brad Smith, 'Microsoft announces new European digital commitments' (*Microsoft blog*, 30 April 2025) <https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/> accessed 2 November 2026.
[41] Article 18 CADA proposal with reference to Article 45 GDPR.

- Union assurance level 4, which requires that the provider not be subject to any control by a third-country government or entity, seems the most insurmountable for third-country cloud providers to meet, yet not impossible. Some argue Big Tech could still meet it by demonstrating European locality and a formal separation between the EU subsidiary and the American parent company, as the decisive criterion is "control" rather than ownership.[42] Either way, this concerns the 1% of public sector activities, as mentioned above.
- For Union assurance levels 2-4, generated data cannot be used for training or fine-tuning AI systems operated by a legal entity established in a third country. While this might seem like a strict safeguard against third-country cloud service providers, security bodies that are subject to these levels already follow strict protocols, while some might even be willing to share such data in exchange for security AI tools.
- Furthermore, once adopted, CADA would become *lex specialis* to the forthcoming Public Procurement Act, proposed in September 2026.[43] That means that it will not be possible to exclude providers from third countries at Union assurance levels 1 and 2, notably from the United States (US).[44] 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,"[45] public sector bodies in the Member States will not be able to adopt or maintain rules that deviate from CADA. 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 light of the above 70% European market share concentrated among three US hyperscalers (Microsoft, Amazon, and Google) at Union levels 1 and 2, in order to reduce dependencies and increase supply chain security and economic security more broadly.
- Besides, these criteria largely neglect the materiality of computing beyond data centre location. The EU largely depends on other countries for chips and raw materials needed for computing.[46] While other legislative initiatives are intended to bridge that gap, including the EU Chips Act 2, proposed with the EU Tech Sovereignty Package, and the Critical Raw Materials Act, their success is also questionable given the geopolitical and physical realities of extracting and producing such materials.[47]

---

[42] Cecilia Rikap and Vali Stan, 'Does Europe Really Have a Plan for Tech Sovereignty?' (*Tech Policy Press*, 29 June 2026) <https://techpolicy.press/does-europe-really-have-a-plan-for-tech-sovereignty> accessed 2 November 2026.

[43] 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, p 5-6.

[44] 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 2 November 2026.

[45] Public Procurement Act proposal, p 7 and case-law cited in fn 11.

[46] See for example Mario Draghi, 'The Future of European Competitiveness - Part B | In-Depth Analysis and Recommendations' (2024) <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059> accessed 2 November 2026, p. 46, 86.

[47] See for example European Court of Auditors, 'Special report 12/2025: The EU's strategy for microchips – Reasonable progress in its implementation but the Chips Act is very unlikely to be sufficient to reach the overly ambitious Digital Decade target' <https://www.eca.europa.eu/en/publications?ref=sr-2025-12> accessed 2 November 2026; Draghi (2024) p. 53.

- **Autonomy and sovereignty narrowly defined:** The Commission Communication accompanying the EU Tech Sovereignty Package provides for an understanding of technological sovereignty as "Europe's ability to develop, control and scale the critical technologies, infrastructure, services and data, including digital ecosystems, that underpin its economy, security and society, while derisking and diversifying supply chains and technological exposure to reduce strategic dependencies and resist foreign interference."[48] Most emphasis is placed on remaining open to the world. The underlying tension is that the EU seeks to reassure openness and continuity in international trade and market relations whilst superficially addressing the almost complete dependence on US tech and infrastructure. Accordingly, the CADA proposal regulates autonomy through the lens of data localisation, protection and security. These sovereignty criteria might seem like they mitigate this dependence whilst, in reality, they are largely performative. While this emphasis on data localisation and securitisation points to US dependence, besides largely failing to address such dependence, it also creates tunnel vision. The CADA proposal turns digital sovereignty into information-security risk regulation that steers away from promoting a European digital stack by strategically leveraging public procurement. Alternative visions of digital sovereignty instead focus on the power to exert influence over digital assets and their governance, including decisions on the purposes for which data are used, the types of technologies through which data are processed, and the infrastructure required to process such data.[49]

E. Cloud federation & open source

- **Operational autonomy left undefined:** With or without the provision of cloud services by European providers, a stranglehold over computing remains. This is a technical feature of cloud computing, i.e., the providers have the technical ability to exercise an unprecedented level of control compared to other (and older) modalities of computing provision. The CADA proposal seeks to enhance computing sovereignty and operational autonomy by territorialising data centres.[50] Interestingly, operational autonomy is neither clarified nor used consistently; on the one hand, the main text refers to the operational autonomy of public sector bodies entrusted with public order tasks.[51] In that way, ensuring operational autonomy serves as a means for preventing "harm that could undermine public order."[52] On the other hand, Annex II refers to the operational autonomy of the cloud service provider under level 1, which the required technical and organisational measures should not compromise. It needs to be further clarified what operational autonomy is and how it can be put into effect. This relates to valid concerns

[48] Communication from the Commission to the European Parliament, the Council, the European Economic and Scial Committee and the Committee of the Regions on European Tech Sovereignty, accompanied by an EU Open Source Strategy, Brussels, 3.6.2026, COM(2026) 503 final.
[49] Bart Anthony Kamphorst and others, 'Opaque Procurement: How Transparency Deficits Compromise Democratic Digital Sovereignty' (2026) 26 Journal of Responsible Technology 100178 <https://doi.org/10.1016/j.jrt.2026.100178>; Margarita Padilla, 'Technological Sovereignty: What are we talking about?' in *Technological Sovereignty Vol. 2* (2017) 5 <https://sobtec.gitbooks.io/sobtec2/content/en/>.; Plixavra Vogiatzoglou, 'Digital-Sovereignty-as-a-Service under EU law', Working Paper (2026).
[50] Recital (5) CADA proposal.
[51] CADA proposal, p. 3.
[52] Ibid.

about operational discontinuity in cloud services, which have been highlighted, and may require governance beyond data centre investment.

- **Cloud federation needs to establish clear control over resources.** CADA suggests an interesting technical design in the form of cloud federations. It is understood as a technical entity that brings together national and European cloud initiatives that provide highly trusted and secure public-sector cloud capabilities and facilitates sharing those capabilities between Union entities and public-sector bodies.[53]
  - Under Title IV, Chapter III, resource sharing involves the "sharing entity", "using entity", and an "intermediate legal entity." Article 35(1) details the sharing process, which requires the sharing entity to own the hardware resources, directly or indirectly. It does not explain the parameters of indirect ownership of hardware resources; instead, here too, control (as described above) is the decisive factor. As per Article 35(1), resources can be federated only if they are owned. This does not translate well to the cloud computing context because it is difficult to establish ownership of hardware resources when using cloud services. Imagine, for example, entity A is the sharing entity which contracted for cloud services. In this case, the cloud service provider is the owner of the resources and the intermediary legal entity. In this case, indirect ownership can only arise if the sharing entity exercises "decisive influence" over the cloud service provider. The CADA proposal needs to explain what this could mean. Otherwise, it will not effectively permit sharing of contracted cloud services. It largely permits sharing of resources directly owned by entities with a concurrent, well-functioning regime for AI workloads, such as the EuroHPC Joint Undertaking Regulation.[54]
  - Furthermore, the cloud federation needs to be distinguished from previous and ongoing attempts at federation such as GAIA -X, EOSC and e-Grids, to name a few, to understand what worked and what did not. This will allow developers to understand whether it is a credible alternative that could be given a legal form and governance structure as a European Digital Infrastructure Consortium.[55]

- **The technical reality of current Open-Source Software (OSS) production needs to be engaged with.** The CADA proposal places a specific focus on OSS as a lever to boost technological sovereignty, in line with the EU Open-Source Strategy 2020-23, which aims to promote open European alternatives across the European technology stack. Article 2(25) defines an open-source license as "a license whereby the reuse, redistribution and modification of software is permitted for all uses on the basis of a unilateral declaration by the right holder that may be subject to certain conditions, and where the source code of the software is made available to users indiscriminately."[56] Thus, the availability of source code is a *sine qua non* condition for software to be designated as open source. However, today, most open-source

[53] Recital (69) CADA proposal.
[54] Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488, OJ L 256, 19.7.2021, pp. 3–51.
[55] Recital (24) CADA proposal.
[56] Article 12 Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), OJ L, 2024/903, 22.3.2024.

development and deployment also run through cloud environments.[57] This has a notable impact on the source code because it is situated on a remote server. Even when code is stored in Git repositories, it is stored online. It must be modified, downloaded, and then run on on-premises systems. Legal scholarship and the Free Software Movement clearly establish the difficulty of accessing source code.[58] This matters because it is not separate from cloud computing. Instead, it uses cloud infrastructure at each step. In this sense, OSS is not the antidote to cloud software services (SaaS). On the one hand, the Commission takes demand-side measures to boost cloud adoption within its Cloud Strategies and the CADA proposal; on the other, it seeks to encourage OSS use. These are two mutually exclusive solutions given the technical realities. The Commission needs to engage with and address this tension.

[57] Fontana, Richard, 'Cloud Native Development, Containers, and Open Source Licensing', in Amanda Brock (ed.), *The Business of Open: Economics, Open Source Models, and Usage* (Oxford, 2022) <https://doi.org/10.1093/oso/9780198862345.003.0020>.

[58] 'The Only Major Threat to Open Source Software License Models like the GPL Is the Spread of "Cloud Computing" and Software as a Service (SaaS) Business Models.' (*My GNU/Linux*, 2011) <https://www.mygnulinux.com/?page_id=866> accessed 2 November 2026; See also GNU Affero General Public License (2007) <https://www.gnu.org/licenses/agpl-3.0.html> accessed 2 November 2026.