Digital Council

Digital Council Position on the Cloud and AI Development Act

Digital Council

Introduction

Digital Council supports the core ambition of the proposed Cloud and AI Development Act (CADA). Europe needs more computing capacity, faster and more predictable permitting for data centres, a more competitive cloud ecosystem, and a trusted framework for protecting critical public services and sensitive government functions.

The European Commission presented the CADA proposal on 3 June 2026. The proposal is at the beginning of the ordinary legislative procedure; as at the cut-off date, neither the European Parliament nor the Council had adopted its negotiating position.[1]

The capacity and innovation provisions of the proposal are largely moving in the right direction. Digital Council particularly supports the provisions concerning data centre acceleration zones, single points of contact, more predictable permitting, and the possibility of designating certain planned data centre projects as strategic. These measures could remove some of the barriers currently holding back investment in European data centres. Success will, however, depend primarily on the availability of electricity, grid capacity, transparent connection rules, and access for businesses and research institutions to the newly created computing capacity.

The proposed framework of four cloud sovereignty levels requires more substantial changes. Strict requirements are legitimate for defence, internal security, justice, and other genuinely critical activities. They should not, however, automatically apply to routine administrative and support systems in public administration.

The proposal requires non-critical public-sector activities to use cloud services recognised at least at Level 1. The conditions for that level include locating the relevant infrastructure in Europe and storing customer data, metadata, and telemetry exclusively in the EU, unless the public-sector customer expressly provides otherwise.[2] Digital Council considers European data residency for customer data at Level 1 to be a legitimate means of supporting the European cloud and AI ecosystem, investment, and knowledge transfer. Such a rule should not, however, be automatically extended without further distinction to all metadata, telemetry, and operational data, irrespective of their sensitivity, technical function, and security purpose.

Another serious implementation risk is the maximum twelve-month migration period where a risk assessment gives rise to a need to change cloud services. Complex public-sector systems may require a new procurement procedure, modifications to integrations, data migration, security testing, and parallel operation. A universal one-year limit could therefore jeopardise the continuity of the very services that the proposal is intended to protect.[3]

Digital Council advocates **open technological sovereignty** based on the ability to choose, control over data, interoperability, security, operational continuity, and the ability to change suppliers. Europe should develop its own technologies and capacity, but should not isolate itself from trusted international partners or restrict access to the best available solutions in the absence of a specific and substantiated risk.

Digital Council therefore supports the strategic direction of CADA, but recommends substantially strengthening the proportionality of the sovereignty framework, revising the approach to Level 1, extending migration periods, respecting Member States' responsibility for national security, preventing fragmentation of the internal market, limiting the expansion of obligations through secondary legislation, and ensuring genuine mutual recognition of audits.

www.digitalcouncil.eu
prague@digitalcouncil.eu

Digital Council, z.ú.
Arbesovo náměstí 257/7, 150 00 Praha 5
IČO: 240 08 389

Digital Council

Digital Council's Priority Recommendations

1. Distinguish between routine and genuinely critical functions

Higher sovereignty levels should be required only for specific services and workloads whose disruption or disclosure could seriously endanger security, public order, or the continuity of the State's essential functions.

2. Establish Level 1 as an open European standard

Level 1 should be based primarily on cybersecurity, transparency, portability, access management, customer control, and European data residency for customer data. The exclusive localisation in the EU of all metadata, telemetry, and operational data should not, however, be an automatic requirement for all routine public-sector systems without regard to their sensitivity and technical function.

3. Recognise equivalent technical, organisational, and legal safeguards

Encryption, customer-managed keys, separate European governance of the service, controlled remote access, a transparent subcontracting chain, and independent audits may in many cases provide more effective protection than geographical, ownership, or formally jurisdictional criteria alone.

Extraterritorial legal risks must be taken seriously. They should not, however, be addressed solely through the provider's place of establishment, the origin of its capital, or its ownership structure. The decisive factor should be the customer's effective control over data, keys, access, operations, audits, and legal safeguards.

4. Extend migration periods

The baseline period should be at least 24 months. For critical or technically complex systems, it must be possible to approve a timetable of at least 36 months, or a longer individual timetable reflecting procurement, testing, security, and service continuity.

www.digitalcouncil.eu
prague@digitalcouncil.eu

Digital Council, z.ú.
Arbesovo náměstí 257/7, 150 00 Praha 5
IČO: 240 08 389

5. Respect Member States' responsibility for national security

A common European methodology is needed. It may be complemented by a model catalogue of public services and workloads in order to reduce fragmentation of the internal market. The Commission's power to change a level determined by a Member State must, however, be exceptional, precisely defined, and accompanied by procedural safeguards. In matters falling within national security, the Commission should primarily play a methodological and coordinating role.

6. Do not extend obligations to the private sector in an open-ended manner through secondary legislation

Potential obligations for the energy, transport, healthcare, banking, or digital infrastructure sectors may be legitimate where genuinely critical infrastructure is concerned. They must, however, be clearly defined in the legislative text itself, supported by an impact assessment, and aligned with NIS2, DORA, and sector-specific rules.

7. Introduce the “one audit – many uses” principle

Audits and evidence submitted under CADA, European certification schemes, and national cloud frameworks should be mutually recognised. Duplicate assessments should be permitted only where they address a specific additional risk.

8. Support European added value without closing the market

Public procurement criteria should reward European research, innovation, jobs, interoperability, security of supply, and SME participation. A company's place of establishment, the origin of its capital, or its formal ownership structure are not, in themselves, sufficient indicators of genuine value for Europe.

Digital Council

1. Why CADA Is Needed

Cloud services, data centres, and accelerated computing have become essential infrastructure for the European economy. The availability of computing capacity affects businesses' ability to deploy AI, the opportunities available to European research, the quality of digital public services, and the security of critical systems.

The Commission's proposal responds to limited and geographically concentrated data centre capacity, the weaker position of European cloud providers, and the legal and operational risks associated with dependence on a limited number of suppliers. CADA therefore combines support for research and innovation, infrastructure development, public procurement, and a new cloud sovereignty framework.[4]

Digital Council agrees with the Commission's underlying diagnosis. Europe needs greater European capacity, more competitive providers, and a stronger ability to protect sensitive systems. Market share, the supplier's country of origin, or the formal location of infrastructure are not, however, reliable measures of security.

Technological sovereignty should be assessed according to the customer's actual ability to:

- control data, access permissions, and encryption keys;
- ensure operational continuity and recovery;
- transfer data and services to another provider;
- use open standards and interoperable architecture;
- independently verify legal, technical, and organisational safeguards;
- avoid disproportionate dependence on a single supplier.

Sovereignty understood in this way is compatible with an open market. Europe can develop its own technologies while cooperating securely with trusted partners. An excessively broad concept of sovereignty could, by contrast, deprive Europe of access to cutting-edge technologies that are also important for developing independent European solutions.

2. Data Centres: The Right Ambition, Challenging Implementation

CADA provides for data centre acceleration zones, single points of contact, and a permitting process of no more than twelve months following the submission of a complete application. When selecting zones, Member States are to consider energy capacity, connectivity, the use of waste heat, environmental impacts, and the potential use of brownfield sites.[5]

Digital Council supports this part of the proposal. More predictable permitting can reduce investment uncertainty and help expand Europe's computing capacity. Administrative acceleration alone will not, however, resolve shortages of electricity and grid connections.

Acceleration zones should therefore be linked to:

- a credible plan for developing the electricity grid;
- transparent information on available and reserved capacity;
- measures against speculative reservations of grid connections;
- flexible consumption, energy storage, and on-site generation;
- the use of waste heat and a preference for brownfield sites;
- high-speed connectivity;
- a measurable contribution to the European technology and research ecosystem.

New data centres should not be assessed solely by installed power capacity or investment volume. Support for strategic projects should also take into account the availability of computing capacity for European businesses, startups, research organisations, and public administration. Otherwise, Europe may formally increase infrastructure capacity without creating sufficient access to computing resources for the entities that are expected to form the foundation of European innovation.

3. The Sovereignty Framework Must Be Proportionate

The proposed Regulation pursues the legitimate objective of strengthening the European Union's digital sovereignty and increasing the public sector's resilience to security risks. At the same time, there is a significant risk that an overly broad

framework would create a separate technology market for the public sector, with adverse effects on competition, innovation, and the functioning of the internal market.

Many software and digital service providers now build their products on standardised cloud platforms and cloud services that are used not only as infrastructure, but also as a source of database, analytics, security, and AI capabilities. If technologically distinct solutions are required for the public sector, suppliers may have to redesign application architectures, replace the cloud services they use, and establish separate operating processes, security audits, and support arrangements.

This risk is particularly significant for startups and small and medium-sized enterprises. Their competitive advantage lies in their ability to develop products rapidly using standardised cloud services. The obligation to operate a separate architecture solely for the public sector may outweigh the economic benefit of participating in public procurement. Many innovative companies could therefore decide not to serve the public sector at all, or to participate only as subcontractors to large systems integrators.

The result could be less competition, higher costs for the State, lower-quality digital public services, and reduced participation by innovative companies, contrary to CADA's objective of supporting the European digital ecosystem and SME participation in public procurement.

The European Commission should therefore expressly assess the proposal's impact on startups, small and medium-sized enterprises, and the cross-border provision of digital services. Cloud sovereignty requirements should be derived from the actual sensitivity of the specific data, services, and workloads concerned, rather than applied indiscriminately to entire organisations or entire information systems.

3.1 Common Levels Can Reduce Fragmentation

CADA introduces four assurance levels. Level 1 is based on the provider's self-assessment of conformity, while higher levels require an independent audit and recognition by the competent authority. Recognised services are to be listed in a common European register.[6]

A single framework can replace divergent national definitions and open a broader European market to providers. That benefit will, however, be lost if Member States begin adding their own requirements, audits, and procedures.

The final Regulation should therefore ensure full mutual recognition, common audit evidence, and a prohibition on national gold-plating in areas covered by CADA. The

purpose of the European framework should be to reduce fragmentation, not to shift it from the national level into parallel certification, audit, and procurement procedures.

3.2 Level 1 Should Not Be a Blanket Rule for All Data and Operational Information

The conditions for Level 1 include locating the relevant infrastructure in Europe and storing customer data, metadata, and telemetry exclusively in the EU, unless the public-sector customer expressly provides otherwise. Public contracting authorities are also to use this level for services that have not been assessed as relevant to the protection of public order.[7]

Digital Council recommends reformulating Level 1. The baseline European standard should primarily require a high level of cybersecurity, transparency regarding location and access, European data residency for customer data, encryption, portability, and continuity plans.

At Level 1, European data residency for customer data is a legitimate means of supporting the European cloud and AI ecosystem. Metadata, telemetry, and operational data should, however, be assessed differently. Such data may vary in sensitivity and technical function, including security monitoring, operational support, incident detection, and ensuring service availability.

Exclusive European localisation of metadata and telemetry should be required where justified by the nature of the data, a specific risk, or a decision by the public-sector customer. For routine systems, it must also be possible to use equivalent technical, organisational, and legal safeguards, in particular transparency, data minimisation, purpose limitation, auditability, encryption, customer control, and access restrictions.

3.3 Effective Control and Extraterritorial Legal Risks

The debate on cloud sovereignty inevitably concerns the extraterritorial reach of foreign legislation, in particular the US CLOUD Act. Digital Council considers these risks legitimate and relevant. They should not, however, lead to the mechanical conclusion that security can be assessed solely by reference to the provider's place of establishment, the origin of its capital, or its ownership structure.

The decisive concept should be effective control. This includes, in particular, who has actual access to data, who manages encryption keys, how remote access is governed, how European operating processes are separated, what legal commitments the

provider makes to the customer, and what options the customer has for audit, control, portability, and termination of the service.

This approach also helps prevent so-called “sovereignty washing”: a situation in which a service is presented as sovereign solely on the basis of a marketing claim, a local address, or a formal partnership, without the customer having genuine control over data, access, operations, and the ability to change suppliers.

3.4 Higher Levels Should Protect Genuinely Critical Services

Stricter requirements may be legitimate for defence, intelligence, internal security, criminal proceedings, or systems whose failure would directly endanger the State's essential functions.

At Level 4, the proposal already moves partly towards protecting genuinely critical services. This principle must, however, be expressly preserved when systems are classified in practice, and its extension to entire organisations or complex systems without distinguishing between workloads must be prevented.

A higher level must always be:

- linked to a specific service or workload;
- based on a substantiated risk;
- limited to what is necessary;
- reviewed regularly;
- accompanied by an assessment of the availability of appropriate solutions on the market.

CADA should support system segmentation, multi-cloud, and hybrid architectures. Requiring an entire complex system to meet the highest level may be more costly and less resilient than dividing its components according to actual risk.

For the most critical services falling within Level 4, a requirement for an operator under European control may be justified. It must, however, be precisely limited to genuinely critical workloads and should not be automatically carried over to lower levels or routine public procurement.

3.5 A Common Methodology Must Neither Undermine Subsidiarity nor Fragment the Internal Market

Member States are to regularly assess public-sector activities using cloud services and determine the corresponding assurance level. The Commission is to prepare a common methodology and, under the proposal, may specify a different level by implementing act if it considers the national assessment inappropriate.[8]

A common methodology is important for the internal market. Without sufficiently harmonised criteria, the same or similar public services could be classified differently across Member States. Information systems for local government, healthcare, education, tax administration, or administrative functions could therefore fall within a lower level in one State and a significantly stricter regime in another.

This would complicate the cross-border provision of services, increase compliance costs, weaken the emergence of a European market for cloud and AI services, and create uncertainty for public contracting authorities and suppliers. Digital Council therefore supports common European criteria, a single methodology, and an indicative model catalogue of public services and workloads.

At the same time, national security judgement must not be replaced by routine Commission decision-making. The Commission's power to change a classification determined by a Member State should be limited by clear legal criteria, mandatory consultation with the Member State, protection of sensitive information, a duty to state reasons, and the possibility of judicial review. In matters directly falling within national security, the Commission should issue recommendations rather than automatically binding decisions.

3.6 Migration Periods Must Reflect Operational Reality

The proposal requires migration triggered by a new risk assessment to be completed within no more than 12 months.[9]

Such a period may be insufficient even for a new procurement procedure, let alone for the secure migration of a complex information system. Large public-sector systems may require changes to application architecture, data migration, integration work, security testing, performance validation, parallel operation, and user training.

Digital Council recommends a baseline period of at least 24 months and, for critical or technically complex systems, the possibility of a timetable of at least 36 months or a

longer individual plan. The period should begin only when a suitable recognised alternative is available. The competent authority must be able to approve a longer timetable where accelerated migration would jeopardise the continuity, security, or integrity of a public service.

3.7 The Private Sector Requires Clearer Delimitation

Article 31 allows the Commission, by delegated act, to impose assessments and measures on private entities in highly critical sectors as well.[10]

Digital Council recognises that certain private entities, for example in the energy, transport, healthcare, banking, or digital infrastructure sectors, perform functions that are essential to the security and continuity of society. It is therefore legitimate to assess whether and how certain CADA requirements should apply to them.

Such an extension must not be open-ended. If obligations for private entities in highly critical sectors are to form part of CADA, their scope, criteria, procedural safeguards, and relationship with NIS2, DORA, and sector-specific rules must be clearly defined directly in the basic legislative text and supported by an impact assessment. The objective should not be a new and duplicative compliance regime, but a clear supplement to existing rules where genuinely necessary.

In the financial sector in particular, DORA already establishes a harmonised framework for digital operational resilience, ICT risk management, and oversight of critical ICT third-party service providers.[11] CADA should therefore not create a duplicative or conflicting regime, but should build on existing sectoral frameworks.

4. Public Procurement and the European Ecosystem

CADA introduces a European added value criterion for innovative cloud and AI procurement. The criterion is to be linked to the subject matter of the contract, disclosed in advance, and remain supplementary rather than decisive.[12]

Digital Council supports this principle. European added value should reward in particular:

- research, development, and intellectual property created in the EU;
- skilled jobs;

- the security and diversification of supply chains;
- interoperability and open standards;
- the participation of European startups and SMEs;
- the integration of technologies originating from European research.

The criteria should not be based solely on a company's place of establishment or ownership structure. Such an approach could disadvantage European scale-ups with international investors and companies that operate successfully in global markets.

Particular attention should be paid to "foreign control" criteria. If interpreted too broadly—for example, by reference to a company's international management, access to non-European financing, presence in non-European markets, revenue from foreign customers, shareholder structure, listing on international stock exchanges, registration of part of its intellectual property outside the EU, cross-border data flows, or employment of non-European workers—the resulting effect could work against European technology companies with global ambitions.

Europe needs companies that are able to grow, raise capital, enter global markets, and compete outside the EU. Foreign-control criteria must therefore be clear, narrow, reviewable, and focused on the actual ability of a foreign State or entity to compel access, influence operations, or disrupt service continuity. They should not penalise European companies for being successful, export-oriented, or financed from international sources.

The proposal also sets a target for innovative SMEs to be awarded at least 25% of relevant public contracts for cloud and AI services.[13] This target should primarily be supported by changes in procurement practice: dividing contracts into lots, using modular architectures and open APIs, setting proportionate turnover requirements, supporting the cost of a first audit, and limiting excessively complex framework agreements.

The EuroCloud Federation and joint procurement can help the public sector share capacity and aggregate demand. They must, however, include competitive safeguards, transparent accounting, and open access for multiple suppliers. Excessively large framework agreements could increase market concentration and close the market to smaller providers.[14]

Digital Council also supports the use of open standards and open-source software. Open source must, however, be accompanied by funding for security audits, maintenance, and professional support. The appropriate principle is **open source first**, not **open source only**.

5. Relationship between CADA and Existing Frameworks

CADA is not being developed in a vacuum. It will apply alongside the European cybersecurity certification framework, national cloud rules, NIS2, DORA, public procurement rules, data protection rules, and forthcoming or parallel regulation of digital infrastructure.

Regulation (EU) 2019/881, the Cybersecurity Act, established the European cybersecurity certification framework for ICT products, services, and processes.[15] CADA should be fully aligned with that framework. Where a provider has already been audited or certified under a European certification scheme, CADA should not require duplicate evidence of the same matters.

The same logic applies to DORA. The financial sector is already subject to harmonised digital operational resilience rules, including ICT risk management and oversight of critical ICT third-party service providers.[16] CADA must prevent overlaps and conflicting requirements that would increase compliance costs without delivering a corresponding security benefit.

CADA must also be considered together with the debate on digital infrastructure, in particular the Digital Networks Act. The development of AI, cloud services, and data centres will not be possible without available energy, connectivity, permitting capacity, and resilient networks.[17] Rules for cloud and AI infrastructure should therefore not be developed separately from broader digital networks policy.

In the Czech context, alignment with the cloud computing catalogue and the existing system of security levels is particularly important. The catalogue publishes cloud computing offerings that have met the requirements of Act No. 365/2000 Coll. for inclusion in the cloud computing catalogue, and public authorities may use the registered offerings in accordance with the ZoISVS rules.[18] NÚKIB also describes Czech cloud computing regulation as an interconnected system comprising the Act on Information Systems of Public Administration, the Cybersecurity Act, and the related cloud decrees.[19]

The final CADA should therefore contain clear transitional mechanisms and recognition rules for national systems. Providers and public contracting authorities should not have to undergo two parallel assessments of the same risks.

Digital Council

6. Priorities for the Czech Republic

CADA can bring new investment to the Czech Republic, provide access to European computing capacity, and create opportunities for Czech providers of cloud, cybersecurity, and software services. At the same time, it will place significant implementation demands on public administration.

The Czech Republic already uses its own system of security levels and a catalogue of cloud services. Aligning the Czech and European frameworks must therefore be a key priority. Providers and public contracting authorities should not have to undergo two parallel assessments of the same risks.

It is equally important to align CADA with existing European and sector-specific rules, in particular NIS2, DORA, European certification schemes, and the forthcoming rules for digital infrastructure. The Czech position should promote the "one audit – many uses" principle and prevent duplicative compliance where comparable technical, security, or sectoral requirements already exist.

During the legislative negotiations, the Czech Government should:

1. compare the European levels with Czech security rules;
2. map public-sector systems and existing cloud contracts;
3. preliminarily identify which systems may require a higher level;
4. estimate the costs, capacity, and time required for potential migrations;
5. prepare a common position of the responsible ministries, DIA, and NÚKIB;
6. analyse suitable locations for data centres on the basis of energy availability, connectivity, brownfield sites, and the use of waste heat;
7. consult providers, public contracting authorities, SMEs, the energy sector, and research organisations on the proposal;
8. prepare public procurement principles supporting modularity, open APIs, and SME participation;
9. develop a transition plan to align the cloud computing catalogue with the future European register;
10. promote the "one audit – many uses" principle at both European and national level.

The Czech position should combine support for European capacity with an emphasis on proportionality, legal certainty, and feasibility. The objective should not merely be to change the structure of public procurement, but to enable safer and faster modernisation of government and create better conditions for the growth of Czech technology companies.

Digital Council

The Czech Republic should particularly advocate that technological sovereignty not be interpreted as isolation from transatlantic partners. For an open economy, it is important to strengthen European capacity while maintaining access to the best technologies, capital, know-how, and security cooperation with trusted partners.

www.digitalcouncil.eu
prague@digitalcouncil.eu

Digital Council, z.ú.
Arbesovo náměstí 257/7, 150 00 Praha 5
IČO: 240 08 389

Digital Council

Conclusion

The Cloud and AI Development Act comes at a time when Europe needs to increase investment in computing infrastructure, accelerate AI adoption, and reduce critical unilateral dependencies. Its strategic direction therefore deserves support.

The final Regulation must not, however, conflate sovereignty with isolation, localisation with security, or restrictions on competition with innovation. Strict requirements should be concentrated on services for which they are genuinely necessary. Routine public administration must have access to secure, modern, and competitive technologies.

At Level 1, European data residency for customer data can be a reasonable means of supporting the European cloud and AI ecosystem. It should not, however, be automatically extended to all metadata, telemetry, and operational data without regard to their sensitivity and function. At the most critical Level 4, an operator under European control may be legitimate, but only as a narrowly defined security tool for genuinely critical workloads.

CADA must also create genuine opportunities for European startups and SMEs. This requires modular procurement, open standards, accessible audits, and rules that reward genuine European technological and economic activity. Overly broad foreign-control criteria could, by contrast, harm the very European companies that aspire to grow globally.

CADA's success will not be measured by the number of new obligations or the number of services labelled sovereign. What will matter is whether Europe gains more secure and sustainable computing capacity, a broader range of competitive technologies, less dependence on individual suppliers, and more resilient public services.

Europe does not need digital isolation. It needs its own capacity, the ability to choose, control over critical dependencies, and an open ecosystem of trusted partners. The final CADA should be built on these principles.

www.digitalcouncil.eu
prague@digitalcouncil.eu

Digital Council, z.ú.
Arbesovo náměstí 257/7, 150 00 Praha 5
IČO: 240 08 389

Digital Council

Footnotes

[1] European Commission, *Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem*, COM(2026) 502 final, 3 June 2026; European Parliament, procedure 2026/0138(COD), status as at 13 July 2026.

[2] European Commission, COM(2026) 502 final, Article 30 and Annex II, Union assurance level 1.

[3] European Commission, COM(2026) 502 final, Article 29(6).

[4] European Commission, COM(2026) 502 final, Explanatory Memorandum, pp. 1–4.

[5] European Commission, COM(2026) 502 final, Articles 10–14.

[6] European Commission, COM(2026) 502 final, Articles 16–22.

[7] European Commission, COM(2026) 502 final, Article 30(2) and Annex II.

[8] European Commission, COM(2026) 502 final, Article 29(3)–(5).

[9] European Commission, COM(2026) 502 final, Article 29(6).

[10] European Commission, COM(2026) 502 final, Article 31(3).

[11] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

[12] European Commission, COM(2026) 502 final, Article 32.

[13] European Commission, COM(2026) 502 final, Article 33(4).

[14] European Commission, COM(2026) 502 final, Articles 34–40.

[15] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, Cybersecurity Act.

[16] Regulation (EU) 2022/2554, DORA.

[17] European Commission, *The Digital Networks Act*, 21 January 2026.

[18] Digital and Information Agency, *Cloud computing offerings*, cloud computing catalogue under ZoISVS.

[19] NÚKIB, *Strategic Analysis: Cloud Computing*, 15 March 2024.