



An Roinn Fiontar,
Turasóireachta agus Fostaíochta
Department of Enterprise,
Tourism and Employment

Public Consultation on EU proposal for a Cloud and AI Development Act (CADA)

Explanatory Note



1. Background

On the 3rd of June 2026, the European Commission published a proposal for a Regulation establishing a framework of measures for strengthening the EU's cloud and AI ecosystem, investment and infrastructure (the Cloud and AI Development Act (CADA)).

The proposal is based on the view that cloud computing and AI have become critical infrastructure for economic growth, public services, innovation, security and competitiveness. However, the Commission identifies several challenges facing Europe:

- A growing shortage of computing capacity and data centre infrastructure needed to support AI development and deployment.
- A high reliance on a small number of non-EU cloud providers.
- Decreasing market share for European cloud providers.
- Risks relating to technological dependency, operational continuity, data sovereignty and economic security.
- Fragmented national approaches to cloud infrastructure, procurement and deployment across Member States.

The Commission argues that these challenges could limit Europe's ability to benefit from the digital transformation and could leave critical services and data dependent on infrastructure and providers outside EU control.

The full proposal is available to view on the [European Commission website](#).

2. Summary of Proposal

CADA has two overarching goals:

1. To strengthen the competitiveness, innovation capacity and resilience of Europe's cloud and AI ecosystem.
2. To create a more integrated and autonomous European market for cloud and AI technologies.

To achieve this, the proposal seeks to:

- Increase the amount of computing capacity available in Europe.
- Accelerate the deployment of sustainable data centres across the EU.
- Support the development of next-generation cloud and AI technologies.
- Reduce strategic dependence on non-European providers.
- Strengthen Europe's technological sovereignty and operational resilience.
- Promote wider adoption of cloud and AI technologies by businesses and public bodies.
- Encourage the use of open-source technologies and European-developed solutions.

The proposal contains a number of measures to achieve this, which are summarised under three pillars below:

2.1 Capacity and Infrastructure

This pillar seeks to increase and geographically diversify data centre and compute capacity across the EU.

- **Data-centre deployment:** Member States in which data-centre capacity is being deployed would be required to designate data-centre acceleration zones, taking account of grid capacity, connectivity, permitting, climate resilience and environmental considerations, and the ability of the site/area to function sustainably.

- **Accelerated permitting:** Projects within these zones would benefit from facilitated administrative procedures, single information points and a proposed maximum 12-month permitting period.
- **Strategic projects:** The Commission could designate qualifying developments as strategic data-centre projects, including projects that support essential public services, incorporate innovative or sustainable technologies, strengthen EU supply chains or address regional capacity gaps. Projects would be required to meet at least two specified criteria, including:
 - support for public services,
 - sustainability/innovation,
 - energy system benefits,
 - strengthening EU supply chains, or
 - addressing capacity shortages
- **Capacity monitoring:** The Commission would monitor available compute capacity, projected demand and geographic capacity gaps across the Union.

2.2 Research, Development, Innovation and Deployment

This pillar is intended to strengthen European cloud and AI capabilities and increase the adoption of these technologies across the public and private sectors.

- **Cloud and AI Leadership Initiatives:** These proposed initiatives would support areas including energy- and resource-efficient data-centre technologies, open cloud stacks, frontier AI, physical and industrial AI, AI-agent platforms and increased cloud and AI uptake.
- **Cross-border projects:** The initiatives would be implemented through large-scale, cross-sectoral projects and could be supported by EU programmes, joint undertakings and Member State resources.
- **Frontier AI priority projects:** The proposal provides for collaborative projects involving at least three Member States, supported through pooled national and EU computing resources.

- **Experience and Acceleration Centres for AI:** Building on the European Digital Innovation Hub network, these centres would support AI adoption, skills development, access to expertise and computing resources, and the scaling of start-ups and SMEs.
- **Innovative SMEs:** Under the proposal Member States should aim for at least 25% of cloud and AI procurement to be awarded to innovative SMEs.
- **National cloud and AI strategies:** Member States would be required to establish national strategies within one year of the Regulation's entry into force, unless existing strategies adequately cover the proposal's objectives. These strategies would address cloud and AI adoption, research and innovation, sustainable data-centre capacity, high-intensity computing, skills, open technologies, procurement and access to data.

2.3 Sovereignty, Autonomy and Adoption

This pillar establishes a 'Union Cloud Computing Sovereignty Framework' through which the EU intends to address dependencies, strengthen the resilience of public-sector cloud use and use public procurement to support European cloud and AI capacity. The detailed proposal for this framework is contained in **Annex II** of the CADA proposal, available in the downloads section of [this webpage](#). The descriptions below are simplified summaries of the detailed requirements set out in the Annex.

- **Union cloud computing sovereignty framework:** The proposal establishes four, cumulative Union assurance levels for cloud services used by Union entities and public-sector bodies. The levels are intended to provide public sector bodies with different degrees of assurance relating to the location, operation, security and governance of cloud services.
 - **Union Assurance Level 1**

Level 1 establishes a baseline level of EU assurance. Providers must be established in the EU, infrastructure and customer data must generally remain within the EU, and providers must demonstrate compliance with current cybersecurity standards. Transparency regarding subcontractors is

also required. Limited outsourcing of technical or operational support outside the EU is permitted where appropriate safeguards are in place.

- **Union Assurance Level 2**

Level 2 introduces stronger requirements. Providers, relevant subcontractors, infrastructure, assets and personnel involved in delivering the service must be located in the EU. Customer data must remain in the EU, services must achieve at least a “substantial” level of cybersecurity certification, and technical and operational support must be provided exclusively from within the EU. The level also introduces requirements relating to software supply-chain transparency and safeguards where providers are subject to third-country control. Data generated through use of the service may not be transferred outside the EU or used to train AI systems operated by third-country entities.

- **Union Assurance Level 3**

Level 3 builds on the Level 2 requirements and places greater emphasis on sovereignty and security. Personnel involved in delivering the service must generally be EU citizens and may require security clearances where classified information is involved. Providers and subcontractors are, in principle, required not to be subject to the control of third countries or third-country entities, although a limited derogation mechanism is proposed. Technical support must be delivered from within the EU by EU-resident personnel.

- **Union Assurance Level 4**

Level 4 is the highest assurance level. It requires EU establishment, EU-based infrastructure and personnel, and the localisation within the EU of sensitive customer data identified through a risk assessment. Services must achieve a “high” level cybersecurity certification. Providers and subcontractors cannot be subject to third-country control, and operational support must be delivered exclusively from within the EU. Providers must also demonstrate effective control over critical software components and

minimise dependencies that could enable third-country influence over the service.

- **Risk assessment and procurement:** Member States and Union entities would be required to assess which public-sector activities using cloud services contribute to the preservation of 'public order' and assign the appropriate assurance level to those activities. Public bodies would be required to use at least Level 1 services, and higher-level services for activities identified as public-order relevant. Limited derogations would apply where suitable recognised services are unavailable or compliance would entail disproportionate cost.
- **National Competent Authorities:** Member States would be required to designate one or more authorities to administer, supervise and enforce the assurance framework.
- **Audit process for assessment:** service providers may self-assess for Union assurance level 1 under the framework; providers seeking recognition under levels 2-4 would be required to obtain an independent audit to confirm their adherence to the standards.
- **Third-country providers:** Services controlled from certain third countries could become eligible for Level 3, subject to Commission recognition. The conditions include data-protection adequacy, safeguards against unlawful access and service disruption, market openness and reciprocal access to public procurement.
- **European added-value procurement criteria:** Separate from the assurance framework, contracting authorities procuring innovative cloud services and AI systems would be required to include non-price criteria examining the tenderer's contribution to the development of the European cloud and AI ecosystem. These criteria would remain ancillary and should not be decisive in the award of a contract.
- **EuroCloud Federation and common procurement:** The proposal establishes a voluntary European public-sector cloud federation and expands the Commission's ability to procure cloud, AI, software and data-centre services on behalf of participating public bodies.

- **Open source:** The proposal promotes the use and reuse of open-source software by public bodies, supported by an EU Open-Source Solutions Catalogue and a network of Open-Source Programme Offices.

3. Public Consultation Process

Submissions are now being sought from interested stakeholders on the provisions contained within the CADA proposal. Interested parties are invited to send their submissions by email to cada@enterprise.gov.ie by 11 September 2026.

3.1 Consultation Questions

Submissions can relate to any part of the Act and there is no requirement to express a view on the entire Act. For guidance, views are particularly sought on the following questions:

General Views

1. What do you consider to be the principal opportunities and challenges arising from the proposed Cloud and AI Development Act (CADA) for Ireland?

Enterprise, Innovation and Competitiveness

2. How might the proposal affect the competitiveness, growth and innovation capacity of enterprises operating in Ireland?
3. What impact, if any, would the proposal have on SMEs, start-ups and scale-ups in Ireland, including their ability to access cloud, AI and compute resources?

Research, Development and AI Adoption

4. Will the proposed measures support greater development and adoption of cloud, AI, and related technologies in Ireland? Please explain your view.

Cloud and Data Centre Capacity

5. Do you agree with the proposal's objective of increasing European cloud, compute and data-centre capacity? Please give reasons for your answer.
6. What factors should be considered when balancing increased cloud and data-centre capacity with energy, environmental and infrastructure objectives?

Sovereignty and Public Sector Cloud Policy

7. Do you support the proposal's objective of strengthening European cloud sovereignty and resilience? Please give reasons for your answer.

8. Do you consider the proposed assurance framework to be proportionate? Please give reasons for your answer.
9. Do you consider the proposed assurance framework to be practical and achievable to implement? What benefits or challenges do you identify for providers or public bodies in following it?
10. What opportunities or risks could arise from the proposed cloud sovereignty framework and associated public-sector cloud requirements?

Additional Comments

11. Do you have any other comments on the proposal?

Please ensure that you clearly indicate the article number(s) to which your comments relate. Given the breadth of the proposal, this will allow your comments to be considered appropriately. A table of articles for reference is below.

Article numbers	Relevant area
1 - 2	Scope, Objectives and Definitions
3 - 9	Cloud and AI Leadership Initiatives
10 - 13	Data Centre Acceleration Zones
14 - 15	Data Centre Strategic Projects and Capacity Monitoring
16	Scope for a Union Cloud Computing Sovereignty Framework
17	Cloud Providers & National Competent Authority Recognition Process
18	Recognition of 'Associated Third Countries' by the Commission
19	'Conformity self-assessment' process (for Union assurance level 1)
20 - 22	Independent audit requirements, provision for a database (central repository) of recognised providers
23 - 24	Transparency obligations, Enforcement requirements and Application of penalties

25 - 26	Designation of one or more ‘National Competent Authorities’ (NCA) for enforcing the sovereignty framework, and inspection/enforcement powers of same
27 - 28	Co-operation between NCA and the Commission, and between Member States, on investigation and enforcement
29	Undertaking of ‘risk assessments’ to classify public sector uses of cloud services, including high risk and ‘public order’ designations
30	Conditions for public procurement under the sovereignty framework
31	Conditions for private sector entities operating in sectors of high criticality
32 - 33	‘Union added value’ public procurement criteria; targets, reporting and monitoring of procurement to support innovative SMEs
34 - 36	Establishment of Euro Cloud federation and sharing of public sector data centre and cloud computing services
37 - 40	Commission common procurement framework for cloud/AI service, participation of Member States in a Steering Committees,
41 - 44	Preference for open-source solutions, arrangements for sharing of software including a network of ‘Open-Source Programme Offices’
45 – 48	Governance provisions: committee, review, delegation/implementation

3.2 Freedom of Information

Please note that responses to this consultation are subject to the provisions of the Freedom of Information Act 2014. Parties should clearly identify confidential or commercially sensitive information in their submission. However, parties should also note that any or all responses to the consultation are subject in their entirety to the provisions of the FOI Acts and may be published on the website of the Department of Enterprise, Tourism and Employment. The Department will redact any personal information prior to publication.

4. Next Steps

Following analysis of responses from stakeholders, the Department may engage bilaterally with stakeholders to explore certain issues in more detail.

Once the public consultation has concluded, the Department will review all submissions, which will assist in informing the Department on stakeholder perspectives on the various articles contained in the proposal.