Council of the European Union
General Secretariat

PUBLIC

Brussels, 16 June 2026

WK 8757/2026 INIT

LIMITE

TELECOM
CYBER
COMPET
MI
IA
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Claud and AI Development Act (CADA): Presentation

Delegations will find in the annex the presentation given in the Working Pary on 16 June.



Cloud and AI Development Act

European Commission

Cloud and AI Development Act (CADA) – scope

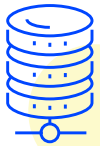
PUBLIC

CADA addresses the need for **homegrown world-class research** and **development** and **innovation (R&D&I)** in AI-enabling technologies, **computing capacity** available across the EU, and **technological sovereignty and competitiveness** in the area of cloud and AI



1 R&D&I

Establishing Cloud and AI Leadership Initiatives, implemented through Grand Challenges, **to boost research and innovation and develop and deploy the next generation of cutting-edge technologies**



2 Capacity

Introducing data centre acceleration zones, permitting predictability and facilitation to **streamline the conditions for the deployment of sustainable data centres across the EU**



3 Autonomy

Creates a single EU-wide assessment and procurement framework for **cloud and AI sovereignty**, **award criteria to foster EU value added**, **joint procurement at the EU level**, MS **federating their infrastructures**, and enhancing the use of **open source**

Pillar 1: R&D&I – Objectives

PUBLIC

Cloud and AI Leadership Initiatives – **General objectives** [Art. 3]

1. Supporting the development and deployment of **cutting-edge cloud & AI technologies**.
2. Reinforcing the Union's **data centre and cloud capacity.**
3. Stimulating the Union's **demand, deployment and uptake** of cloud & AI technologies across the public & private sectors.

Cloud and AI Leadership Initiatives – **Operational objectives** [Art. 4]

1. Advanced data centre technologies
2. Cloud and AI stack
3. Frontier AI
4. Physical AI
5. Industrial AI
6. Platforms for AI agents
7. AI systems and AI models
8. Adoption of cloud and AI across public and private sectors

Pillar 1: R&D&I – Implementation (1/3)

PUBLIC

Grand Challenges [Annex I]

- Operational objectives implemented through **Grand Challenges**
- **Who implements:** Commission, Member States (including EDICs), JUs
- **Funding:** Union programmes, ERDF, RRF
- **Synergies:** Commission and MS shall ensure complementarity with Chips Act 2,Open Source and relevant national and regional strategies

Priority AI projects and compute supports [Art. 8]

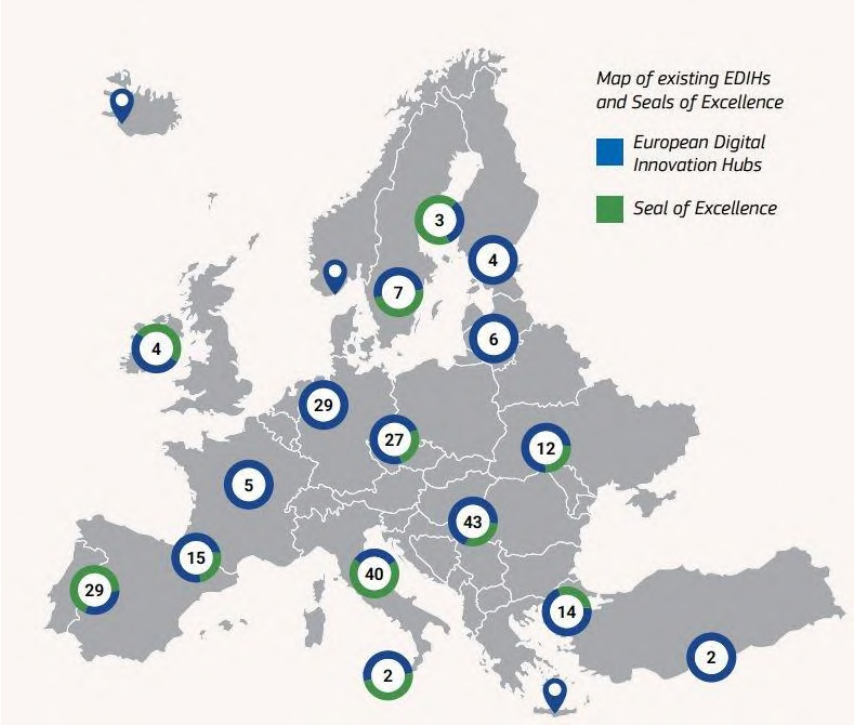
EDICs pioneering **Frontier AI** should have access **to sufficient AI computing resources**, with the EU matching the computing resources provided by MS

Pillar 1: R&D&I – Implementation (2/3)

PUBLIC

Experience and Acceleration Centres for AI [Art. 5]

- Will promote the **broad adoption of AI by private and public sector organisations**, including SMEs and small mid-caps
- Will build on the current network of **European Digital Innovation Hubs (EDIHs)**
- Will be particularly tasked with:
  - ✓ helping organisations accelerate their **digital transformation** through access to and use of AI technologies
  - ✓ **upskilling and reskilling** schemes
  - ✓ facilitating the **transfer of expertise** across regions
  - ✓ supporting the **scaling-up** of spin-offs and start-ups



Pillar 1: R&D&I – Implementation (3/3)

PUBLIC

National Cloud and AI Strategies [Art. 7]

- National cloud and AI strategies include **joint elements to strengthen coordination**, such as:
  - ✓ key **objectives and priorities for cloud and AI adoption**, in line with the 'AI first' principle,
  - ✓ measures to accelerate the development and adoption of cloud and AI **at national, regional and local level**, particularly among public sector bodies, SMEs and SMCs,
  - ✓ measures to support the broad deployment and uptake of AI **in strategic industrial and public sectors**, including in healthcare, energy and mobility,
  - ✓ measures to support the **deployment of data centre capacity**, with a focus on high-value data centres;
  - ✓ measures to support the **development of cloud and AI capabilities** and promote excellence and Innovation;
  - ✓ measures to support the **development of cloud computing stack technologies** strengthening EU technological sovereignty and competitiveness.
- **AI Board to advise and assist Member States** as regards the coordination of national strategies.
- If strategy already exists, an opportunity to identify potential gaps and update accordingly.

Pillar 2: Capacity – Acceleration zones

PUBLIC

Data Centre Acceleration Zones (DCAZ) [Art. 10]

- MS **designate at least one data centre acceleration zone,** having assessed:
  - ✓ Site location and size
  - ✓ Current and future grid capacity, and options for on-site storage and clean energy generation
  - ✓ Current and future network connectivity
  - ✓ Support for phasing out legacy copper networks
  - ✓ Opportunities to reuse data centre waste heat
  - ✓ Measures to accelerate construction and operating permitting
  - ✓ Preference for brownfield over greenfield sites
  - ✓ Environmental sustainability, carbon reduction and climate resilience
- MS **single information point** accompany the DC investor throughout the lifecycle of the data centre project [Art. 12]
- MS **prepare and issue an aggregated baseline permit** for the acceleration zones. Data centres benefit from **facilitated permit granting processes** [Art. 13]
- MS shall **set sustainability requirements** according to indicators specified in Union law and **ensure fair allocation** between operators [Art. 11]

Pillar 2: Strategic data centre projects

PUBLIC

Commission designates strategic projects based on open calls for expression of interest that meet two of the following conditions [Art. 14]

1. Significant contribution to grid stability
2. Supports essential public sector functions
3. Includes highly sustainable and innovative features
4. Incorporates tech produced in the Union
5. Addresses major compute shortage

Benefits

- Access to support from **Union Programmes**
- **Competitiveness Seal** under the European Competitiveness Fund

Pillar 2: Capacity – Monitoring

PUBLIC

Monitoring capacity gap [Art. 15]



Available Compute capacity including edge



Demand for data centre capacity

Pillar 3: Autonomy – Sovereignty 1/4

CADA establishes a **Union cloud and AI sovereignty framework** consisting of **four assurance levels** [Art. 16, Annex II and Annex III]

PUBLIC

	Control	EU infra-structure	Personnel	AI inference data	Supply chain	Sub-contractors	Vulnerability disclosure restrictions	Cybersecurity	Type of assessment
Level 4	EU established, owned and controlled	Fully located in the Union	Located in the EU and EU citizens. Security cleared (**)	Not transferred outside of the EU and not reused by a third-country entity	**Effective control** (over the software)	Established in the Union, owned, and controlled	Not needed	High	National authorities based on a 3rd party-audit
Level 3	EU established, owned and controlled (*)	Fully located in the Union	Located in the EU and EU citizens. Security cleared (**)	Not transferred outside of the EU and not reused by a third-country entity	**High degree of control** (auditable software)	Established in the Union. If owned by a 3rd country, absence of interference (*)	No hidden disclosures	Substantial	National authorities based on a 3rd party-audit
Level 2	EU established & absence of 3rd country interference	Fully located in the Union	Located in the EU. EU citizens if required by the customer	Not transferred outside of the EU and not reused by a third-country entity	**High degree of control** (auditable software)	Established in the Union. If owned by a 3rd country, absence of interference	No hidden disclosures	Substantial	National authorities based on a 3rd party-audit
Level 1	EU established	Fully located in the Union	Located in the EU	No requirement	No requirement	Full transparency	No hidden disclosures	State-of-the-art cybersecurity standards	Self-assessment

(*) a cloud computing service subject to the control of a third country or a legal entity established in a third-country can still be audited against the audit criteria where the third country has implemented specific safeguards that ensure that there is no risk of unauthorised access to Union data or possible disruption of service quality or continuity.

(**) where appropriate

Pillar 3: Autonomy – Sovereignty 2/4

PUBLIC

3rd country recognition [Art. 18]

Where the provider is subject to the control of a 3rd country, the Commission may decide that the **3rd country provides sufficient sovereignty guarantees and reciprocity** allowing the provider to be audited against **Level 3**.

Criteria for the Country:

(a) Existence of a **GDPR** adequacy decision

(b) No measures in place that conflict with the lawful access to non-personal data set out in the **Data Act**;

(c) No measures in place to **degrade or disrupt service continuity or provision**. It also has no **restrictive measures such as sanction regimes, embargoes, or any equivalent legal or administrative measures**, unless these specific measures are legitimate under the national laws of Member States or Union law;

(d) No measures in place to **impede the provision of state-of-the-art technologies and services**;

(e) It maintains **an open market** to Union cloud computing services;

(f) the third country grants **equivalent levels of access to public procurement** procedures to EU companies.

Pillar 3: Autonomy – Sovereignty 3/4

PUBLIC

Recognition of services, mutual assistance and cooperation

MS competent authorities can **recognise** [Art. 17], **after consulting the other MS,** services on the basis of evidence provided by the providers and :

1. ***Level 1:*** **Conformity self-assessment** [Art. 19] SME exception under Art.17(3))
2. ***Level 2:***
3. ***Level 3:***
4. ***Level 4:***

Independent third-party audits by auditors assessing conformity against the audit criteria and audit evidence of Levels 2, 3, or 4 provided in CADA [Art. 20 & 21] .

- **Recognised** services are registered in a **publicly available central repository** [Art. 22]
- Provisions for **transparency** [Art.23] and **penalties and compensation** [Art.24]
- Designation of **competent authorities** [Art.25] and their **powers** [Art.26].
- Competent authorities and the Commission **cooperate, exchange information, and assist each other** to enforce the sovereignty framework [Art. 27].
- Where **non-compliance is suspected**, competent authorities can request the competent authorities of establishment to **investigate and take enforcement action** [Art. 28].

Pillar 3: Autonomy – Sovereignty 4/4

PUBLIC

Public sector risk assessment and procurement [Art. 29-30]

- **MS conduct national sovereignty risk assessments** which determine which public sector use cases shall be served by cloud and AI services of Level 1-4
- **Commission shall issue implementing acts providing the methodology** for MS assessments to ensure a convergent application of Levels 1-4 across the Union
- **MS public sector organisations shall use** only services awarded Level 1-4

Private sector essential entities (NIS2 Annex 1) [Art. 31]

- **Private sector essential entities may conduct** an assessment on the basis of MS sovereignty risk assessment criteria to drive their cloud and AI procurement and uptake strategies
- **Commission may** through delegated acts decide which sectors require the assessment and mitigation measures to be taken

Pillar 3: Autonomy – Resilience 1/4

PUBLIC

EU Added Value [Art. 32]

- If contracting authorities use non-price criteria in public procurement of innovative cloud and AI, they **shall apply EU Added Value award criteria.**
- The criteria shall be **non-decisive** and shall **reward** (i) **reinforcing EU supply chain**, (ii) **integration of EU-funded technologies**, (iii) **innovation carried out in the Union**, (iv) **integration of EU hardware.**

Innovation procurement [Art. 33]

- **MS shall monitor and report yearly** on their procurement of innovative cloud and AI services and AI systems and shall set an **objective of 25%** of such procurement is **awarded to innovative SMEs**

Pillar 3: Autonomy – Resilience 2/4

PUBLIC

Public sector cloud federation (EuroCloud) [Art. 34-36]

- CADA establishes a **voluntary public sector cloud federation**
- The EuroCloud Federation enables Union entities and public sector bodies to **voluntarily share their own data centre and cloud capacity** with each other, provided they:
  - ✓ own or control the underlying hardware
  - ✓ ensures secure and resilient service provision
  - ✓ charge only cost-based fees.
- CADA stipulates the criteria which allow participating MS public sector organisations to participate.
- Commission tasked with setting up the platform of exchange

Pillar 3: Autonomy – Resilience 3/4

PUBLIC

Joint procurement [Art. 37-40]

- Commission may carry out **EU-level cloud and AI procurement** on behalf of **EUIBAs, MS contracting authorities and partner organisations**
- Commission would be able to carry out **multiple procurement procedures** (e.g.: joint procurement but also central purchasing activities)

Pillar 3: Autonomy – Resilience 4/4

PUBLIC

Open Source [Art. 41-44]

- MS shall **promote open-source software in public procurement**
- Publish software released in the **EU OSS Catalogue** established by CADA
- Commission shall establish an **OSPO Network**.

PUBLIC

Thank you!

