Council of the European Union
General Secretariat

PUBLIC

Brussels, 07 September 2026

WK 13637/2026 INIT

LIMITE

CYBER

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on cyber issues (attachés)
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) – Interplay between CADA and CSA2 - Presentation

Delegations will find in the annex a presentation given by the Commission at the meeting of the Horizontal Working Party on Cyber Issues on 7 September 2026.



CADA & CSA2

07.09.2026

DG CONNECT

European Commission

Pillar 3: Autonomy – Sovereignty

PUBLIC

CADA establishes a **Union cloud and AI sovereignty framework**

Common **definition of assurance levels** for cloud services

Common **mechanism to recognise assurance levels** of cloud services

Common **approach to use** recognised services focusing on the public sector

Pillar 3: Autonomy – Sovereignty

CADA establishes a **Union cloud and AI sovereignty framework** consisting of **four assurance levels**

	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

PUBLIC

An EU-level approach to cloud cybersecurity is a cornerstone of CADA

PUBLIC

Cybersecurity is **one of the criteria** in the CADA Sovereign Cloud Framework

	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

Cybersecurity criteria in CADA

PUBLIC

*"[…] the audited service obtains a **European cybersecurity certificate of at least assurance level ['substantial'/ 'high'] under a European cybersecurity certification scheme covering cloud computing services to be established under Regulation (EU) 2019/881**, provided that such a scheme has been established under that Regulation and is available to cloud computing service providers. Until the establishment of such a scheme, national cybersecurity certification schemes shall apply, where they exist. Where no Union or national cybersecurity certification schemes exist, the audited provider is to demonstrate that the service complies with the highest cybersecurity standards under applicable Union law; […]"*

Pillar 3: Autonomy – Sovereignty

PUBLIC

3rd country recognition

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

PUBLIC

Recognition of services

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

1. ***Level 1:*** **Conformity self-assessment** (publicly available statement of conformity. SME exception)
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.

- Competent authorities have **investigative powers.** MS and the Commission provide **mutual assistance.**
- **Recognised** services are registered in a **publicly available central repository**

Pillar 3: Autonomy – Sovereignty

PUBLIC

Public sector risk assessment and procurement

- **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)

- **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