Council of the European Union
General Secretariat

PUBLIC

Brussels, 07 July 2026

WK 10169/2026 INIT

LIMITE

TELECOM
CYBER
COMPET
MI
IA
CODEC

REDACTED DOCUMENT ACCESSIBLE TO THE PUBLIC (25.08.2026). ONLY MARGINAL PERSONAL DATA HAVE BEEN REDACTED.

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:	Cloud and AI Development Act: Presentation

Delegations will find in the annex the presentation given in the Working Pary on 7 July.

PUBLIC

Cloud and AI Development Act

07.07.2026

[redacted], Head of Unit – E2 Cloud and Software

European Commission

Union cloud and AI sovereignty framework

PUBLIC

An EU-wide **definition of 4 Union assurance levels** for cloud services

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

A common **approach to procure** recognised service (for the public sector)

Union cloud and AI sovereignty framework

PUBLIC

Key objectives of the Sovereignty Framework

- Strengthen public sector confidence in cloud procurement by introducing a **harmonised definition of sovereign cloud**
- Adopt a **balanced and proportionate approach**, structured around four increasingly sovereign assurance levels
- Assess services through **objective and auditable criteria** addressing the different dimensions of sovereignty, while **minimising administrative burden**
- Ensure an appropriate level **of subsidiarity** by preserving Member State autonomy while **ensuring coherence**
- **Draw inspiration from existing frameworks** such as FedRAMP and the Commission's own sovereign cloud procurement framework (DIGIT).

PUBLIC

Definitions

Definitions (1/2)

PUBLIC

Definition of cloud computing services [Art. 2(1)&(2)]

- **'cloud computing service'** means cloud computing service as defined in Article 6, point (30), of Directive (EU) 2022/2555 **(NIS2 Directive)**;
  - **Recital (10)** further specifies that it **encompasses on-demand access to AI systems** as defined in Article 3, point (1), of Regulation (EU) 2024/1689 (AI Act), hosted and operated remotely. **Only the delivery and making available of an AI system forms part of the service**. The AI system itself and its underlying model are excluded from the scope of this definition.
  - *NIS2 Definition of cloud computing services - **'cloud computing service'** means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;*
- **'cloud computing service provider'** means a legal entity which provides a cloud computing service;

Definitions (2/2)

PUBLIC

Other definitions [Art. 2]

- **'AI system'** means an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 (AI Act);
- **'public sector body'** means public sector body as defined in Article 2, point (1), of Directive (EU) 2019/1024 (PSI Directive);
- **'Union entities'** means the Union institutions, bodies, offices and agencies set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of the European Union (TFEU) or the Treaty establishing the European Atomic Energy Community;
- **'contracting authorities'** means contracting authorities as defined in Article 2(1), point (1), of Directive 2014/24/EU (PPD);
- **'auditing organisation'** means an individual organisation, a consortium or other combination of organisations, including any subcontractors, that the audited cloud computing service provider has contracted to perform an independent audit;
- **'audited service'** means a cloud computing service being audited for the purpose of receiving an audit report and an audit opinion;
- **'audit criteria'** means the criteria, pursuant to Annex II to this Regulation, against which the auditing organisation assesses whether the audited provider and its audited service comply with each cumulative criterion to be met for it to be recognised as offering Union assurance levels 2, 3, or 4;
- **'audit evidence'** means any information used by an auditing organisation to support the audit findings and conclusions and to issue an audit opinion, including data collected from documents, databases or IT systems, interviews or testing performed;

PUBLIC

An EU-wide definition of the 4 Union assurance levels

Title IV: Common sovereignty framework (1/17)

PUBLIC

Scope [Art. 16]

- Article 16 establishes a **Union cloud computing sovereignty framework** comprising **four Union assurance levels (UALs)**
- The criteria of the four Union assurance levels are set out in **Annex II**
- Paragraph 2 empowers the **Commission to adopt delegated acts** to amend **the criteria set out in Annex II** and the **evidence in Annex III**
- To ensure Annex II and Annex III **remain up to date** with new legal or technical developments, paragraph 3 sets the obligation for the Commission to **review the Annexes at least every 18 months**

Title IV: Common sovereignty framework (2/17)

PUBLIC

Criteria (Annex II) and audit evidence (Annex III)

- **Annex II sets out the cumulative criteria** to be met by cloud computing service providers and their services to be recognised as offering services at UALs 1, 2, 3 and 4.
- **'software'** within the meaning of Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 3, point (4) falls within the scope of both Annex II and III, while **'hardware'** within the meaning of Regulation (EU) 2024/2847, Article 3, point (5) is out of the scope.
- **Annex III provides audit evidence** that auditing organisations should request from the audited provider when assessing the compliance of the audited service against the applicable audit criteria under Annex II.
- **N.B.:** Annex III is indicative and does not limit the evidence that may be requested or considered by auditing organisations. Auditors **may seek any additional information necessary to ensure a comprehensive and accurate assessment of compliance** to conduct audits. While the evidence requested may be the same, the aspects that need to be analysed will differ depending on the assurance level criteria and their strictness

Title IV: Common sovereignty framework (3/17)

PUBLIC

Union establishment – Criterion (a)

- For **UAL1** the service provider must be **established in the Union** (= where the service provider has its head office or registered office from which the principal financial functions and operational control are exercised)
- For **UALs 2, 3 & 4** the service provider **+ its subcontractors** must be **established in the Union**

- Under **Annex III**, evidence may include, **but is not limited to**, documentation demonstrating:
  a) that the provider is legally incorporated under EU Member State law
  b) that the registered office, central administration, and main establishment is located in the EU
  c) a genuine and stable EU presence (not just formal registration)
  d) that key operations are EU-based, including offices, staff, customer support, contracting, and finance

Title IV: Common sovereignty framework (4/17)

PUBLIC

Location of infrastructure, assets and personnel – Criterion (b)

- For **UAL1** the **infrastructure + assets** of the service provider and its subcontractors **must be located in the Union** unless explicitly required otherwise
- For **UALs 2-4** the **infrastructure, assets + personnel** of the service provider and its subcontractors **must be located in the Union**, unless explicitly required otherwise

- Under **Annex III**, evidence may include, **but is not limited to**, documentation demonstrating:
  i. infrastructure located in the EU: evidence that all infrastructure, data storage (including backup, disaster recovery, and logs), and network architecture are exclusively Union-based.
  ii. assets located in the EU: evidence that all servers, equipment, and operational capabilities used to deliver the service are in the Union.
  iii. Personnel located in the EU: evidence that staff responsible for delivering the service are in the Union through employment and organisational records.

Examples of what may constitute infrastructure, assets, and personnel:

(a) **Infrastructure:** physical facilities and systems supporting the data centre
(b) **Assets:** hardware, software, internal networks, libraries, and cryptographic materials used
(c) **Personnel:** employees responsible for delivery, administration, security, availability, and operation

Title IV: Common sovereignty framework (5/17)

PUBLIC

Customer data location – Criterion (c)

- **Customer data** (including metadata and telemetry data) that is processed, stored, and transferred by the service provider and its subcontractors **remains exclusively within the Union**, unless explicitly required otherwise by the customer (applicable across levels 1-**4**)

- Under **Annex III** evidence may include, but is not limited to, documentation demonstrating:

a) that customer data are stored and processed exclusively in the Union and that third-parties or subcontractors that do not meet the conditions are in no circumstances technically or operationally able to access, obtain, make unavailable, destroy or more generally process customer data without prior authorisation
b) logs and monitoring records showing that all data are stored and processed exclusively within the Union
c) data flow diagrams showing the flows of data

Title IV: Common sovereignty framework (6/17)

PUBLIC

Customer data location – Criterion (c)

- N.B., under **Annex III** a customer means a public sector body who has entered into a contractual or other legally binding arrangement with the service provider for the purpose of accessing or using the service.
- **'customer data'** could mean any data under the control of the customer, whether by legal, contractual, or other means, that are (a) input into the cloud computing service by or on behalf of the customer, including authentication credentials; (b) produced through the customer's use of the cloud computing service.
- **'customer data'** may also include data under the audited providers control that are derived as a result of interaction with the audited service by the cloud service customer. This includes customer data and any data resulting from the usage of the cloud computing services **(i.e. telemetry, metadata)**.
- **'cloud computing service derived data'** includes the portion of log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorised users and their identities. It can also include any configuration or customisation data, where the cloud computing service has such configuration and customisation functionalities.

Title IV: Common sovereignty framework (7/17)

PUBLIC

Personnel screening and Union citizenship – Criterion (d)

- For **UAL 1** **no personnel screening or citizenship requirement**
- For **UAL 2**, if the Union entity or public sector body determines that imposing **additional personnel screening and Union citizenship requirements** are necessary, the audited provider should ensure that personnel meeting those requirements are available
- For **UALs 3-4**, the **personnel** of the service provider **+ its subcontractors** are **Union citizens** and where appropriate, must also have the necessary **national security clearance**

- Under **Annex III**, evidence may include, but is not limited to, documentation demonstrating:

a) that the provider has implemented the measures to demonstrate valid official government issued documents (e.g. valid passport and national identity card)
b) organisational charts and job descriptions confirming that only personnel with Union citizenship have access to the audited service's operation, management, maintenance, and support
c) access control policies and audit trails showing that only authorised personnel who are Union citizens can access the service's systems and data
d) procedures describing how citizenship is verified before assignment and how compliance is maintained throughout employment

Title IV: Common sovereignty framework (8/17)

PUBLIC

Cybersecurity requirements - Criterion (e)

- For **UAL1** the cloud computing service complies with **state-of-the-art cybersecurity standards**
- For **UALs 2-3** the service complies with **EU cybersecurity certification (≥ substantial)** where established. Otherwise, **national cybersecurity schemes** or **highest applicable EU standards** apply
- For **UAL4** the service complies with **EU cybersecurity certification (= high)** where established. Otherwise, **national cybersecurity schemes** or **highest applicable EU standards** apply

- Under **Annex III**, evidence may include, but is not limited to, documentation demonstrating:

a) a valid cybersecurity certification demonstrating compliance with the applicable assurance level under the relevant European cybersecurity certification scheme
b) Until the EU cloud certification scheme is in place, compliance may be demonstrated through recognised alternative certifications (e.g. CEN standards, national cybersecurity schemes, or equivalent high-level cybersecurity evidence).

Title IV: Common sovereignty framework (9/17)

PUBLIC

Data generated using the service – Criterion (f)

- For **UAL 1 no requirement**
- For **UALs 2-4 the data generated by using the service cannot be used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country** and cannot be transferred outside the Union

- Under **Annex III** evidence may include, but is not limited to, documentation demonstrating:

a) contractual clauses including clauses that data is limited to service delivery only.
b) technical and operational evidence including data flow diagrams, MLOps/deployment records, model/system cards, and lineage documentation showing EU-based processing, full traceability, and no external data transfer or secondary use.
c) Governance and third-party transparency, including data lineage/provenance controls and disclose all subcontractors accessing the data, including their country of establishment.

Title IV: Common sovereignty framework (10/17)

PUBLIC

Control – Criterion (g)

- For **UAL 1** **no requirement on control**
- **Definition of 'control'** → the ability to exercise a **decisive influence** on a legal entity directly, or indirectly through one or more intermediate legal entities (Article 2, point (6) of the European Defence Fund)
- For **UAL 2** if the audited provider **is subject to the control of a third country or a legal entity established in a third country** the necessary **legal, technical and organisational measures must be implemented** to:

i. ensure that the control is not exercised in a manner that restrains or restricts the provider's ability to perform and deliver the service, imposes limitations on the infrastructure, assets, and personnel required for the service provision, or undermines the capabilities and standards necessary to perform the audited service.
ii. prevent access to customer data by the third country or legal entity established in the third country
iii. prevent the possibility of disruption of the service continuity and/or degradation of the service quality
iv. ensure that the control is not exercised in a manner that obliges the audited provider to implement, enforce, give effect to, or comply with restrictive measures such as sanction regimes, embargoes, or any equivalent legal or administrative measures adopted by a third country, unless such measures are legitimate under the national laws of Member States or Union law

Title IV: Common sovereignty framework (11/17)

PUBLIC

Control – Criterion (g)

- For **UAL 3** the audited provider + its subcontractors are **not subject to the control** of a third country or a legal entity established in a third-country.
- **Derogation possible** where provider + subcontractors subject to the control of a third country or legal entity established in a third country can be audited against UAL3 if the **Commission has adopted an implementing act under Article 18**.
- Even with such a decision, the legal, technical and organisational measures under UAL2 apply + **the provider should allow for reasonable access to the code, must be met**
- For **UAL 4** the audited provider + its subcontractors are **not subject to the control** of a third country or a legal entity established in a third-country (**no derogation**)
- Under **Annex III**, evidence may include, but is not limited to:

a) **Ownership check** – mapping the full ownership chain up to ultimate owners.
b) **Governance check** – review board structure, voting rules, and ability to influence or block strategic decisions.
c) **Control beyond ownership** - assessing influence via commercial ties, financial dependencies, or other arrangements.
d) Corporate documents (cap table, shareholder agreements, bylaws, board records) and subcontractor disclosures and management info to identify HQ and executive management locations.

- **If control exists** - proof of legal/technical/organization separation and safeguards
- Auditing organisations must verify and assess the **degree** or **absence of control**.

Title IV: Common sovereignty framework (12/17)

PUBLIC

Control - Associated third countries [Art. 18]

Where the provider is **subject to the control** of a third country or a legal entity established in a third-country, the Commission may decide by means of **implementing acts** that the **third country provides sufficient sovereignty guarantees and reciprocity** allowing the provider to be audited against **UAL 3**.

Criteria for the Country:

(a) Existence of a **GDPR** adequacy decision. Recital (61) specifies that the EC should assess whether the decision applies generally to the third country as a whole or is limited to specific sectors or certified organisations.

(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.

Title IV: Common sovereignty framework (13/17)

PUBLIC

Outsourcing support or assistance outside of the Union – Criterion (h)

- For **UAL1 criterion (d)**, outsourcing of technical and operational support or assistance to third parties outside of the Union is permitted only if the **necessary legal, technical, and organisational measures** are implemented to ensure traceability, security and governance over those operations and they **do not compromise the operational autonomy**
- For **UAL 2 criterion (h),** outsourcing of technical and operational support must occur **exclusively in the Union**
- For **UALs 3-4 criterion (h),** outsourcing of technical and operational support must occur exclusively in the Union + **Union residency of personnel + third parties not subject to the control of a third country or legal entity established in a third country**

- Under **Annex III**, evidence may include, but is not limited to, documentation demonstrating:

a) technical and organisational measures ensure that administrative access to systems used to operate the audited service is provided through access paths located within the Union

Title IV: Common sovereignty framework (14/17)

PUBLIC

Software supply chain – Criterion (i)

- For **UAL 1** **no requirement on software supply chain**
- For **UAL 2-4** the audited provider must demonstrate a complete and up-to-date **Software bill of materials** + list of **dependencies**
- For **UAL 2-3** where **software components or products** are provided, owned, and licensed by a legal entity established in a third country, **controls are implemented and documented** to **block any remote features** that could materially tamper with or disrupt a device, system, or software (including during updates) and to ensure that the **security-relevant components** from third-country manufacturers are subject to **source code audits**, and have a **documented migration plan** in the event that the vendor fails or a third country imposes restrictions;
- For **UAL 4** the audited provider must retain **effective control** over the software components or products by demonstrating that a third country or a legal entity established in a third **country does not hold or exercise effective control over the design, development, maintenance, and evolution of those components or products**.
- Effective control includes the ability to **materially influence** the technical evolution, maintenance priorities, security remediation, and long-term continuity of the component;

Title IV: Common sovereignty framework (15/17)

PUBLIC

No software vulnerability disclosure obligation – Criterion (i) iii

- For **UALs 1 criterion (g), and 2-3 criterion (i) iii,** where the CSP is subject to the control of a third country or third country legal entity, the provider guarantees that there are **no** existing laws and practices in that third country, demonstrated by independent sources, requiring the CSP to **report information on software vulnerabilities** to authorities of that third country prior to those vulnerabilities being known to have been exploited

- This **does not apply to UAL 4** as the service provider **cannot be subject to the control** of a third country or a third country legal entity at this level

Title IV: Common sovereignty framework (16/17)

PUBLIC

Open-source software (j) + Subsidiary in 3rd country (k)

Open-source:

- **UAL 1** → **no requirement** on software released under an open-source licence
- **UAL 2-4** → where the audited provider uses **software released under an open-source licence** it must have implemented and documented the **appropriate controls** to prevent the use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software
- Under **Annex III**, evidence may include, but is not limited to, documentation demonstrating that there is no use of any remote features or mechanisms that could be used to materially tamper with or disrupt a device, system, or software (e.g., change management procedures or up-to-date OSS).

Subsidiary in a third country:

- **UAL 1 - no requirement**
- **UAL 2-4** → to the extent that the audited provider provides its services globally and **maintains a subsidiary in a third country**, it must have implement the necessary measures to ensure and enforce the **effective legal, technical and organisational separation** between the European parent company and any such third-country subsidiary
- Under **Annex III**, evidence may include, but is not limited to, documentation demonstrating that the subsidiary is **legally and operationally independent** from the audited provider + **no access to Union data**

Title IV: Common sovereignty framework (17/17)

PUBLIC

Subcontractors (Annex II points 1.2, 2.2, 3.2, and 4.2)

- For **UAL1** the service provider must ensure **full transparency** of subcontractors and subject them to **due diligence**, **contractual obligations** and **ongoing oversight**

- For **UALs 1&2**, the subcontractors must be **third parties** that have a **direct contractual relationship** with the service provider and **contribute to the provision and the delivery** of the service.

- For **UALs 3&4**, the subcontractors must **third parties** that have a **direct contractual relationship** with the service provider, and **contribute to the provision and the delivery** of the cloud computing service and **may require access to classified** or **sensitive information** to carry out the service provision.

PUBLIC

A Common mechanism to recognise the assurance levels of cloud services

Mechanism to recognise services (1/13)

PUBLIC

Recognition of cloud computing service providers [Art. 17]

- To be recognised as offering a specific UAL, cloud computing service providers shall submit an **application for recognition** to the **national competent authority** (NCA) **of establishment.**

- The NCA of establishment ('the evaluating NCA") may **request the other NCAs to collaborate** in evaluating the application for recognition. NCAs shall accept or refuse the request within 15 days.

- The application for recognition shall contain all the **relevant evidence** required under Article 17.3 or Article 17.4:
  - For UAL 1: the EU statement of conformity.
  - For UAL 2-4: the audit report, the positive audit opinion, and the evidence provided to the auditing organisation.

Mechanism to recognise services (2/13)

PUBLIC

Recognition of cloud computing service providers [Art. 17]

- The NCA of establishment shall review the application for recognition within **60 days**. During this period, NCA of establishment can either:
  - **prepare and notify the draft recognition** decision to the other NCAs, including the required evidence, for a 60-day review period;
  - **request further information** to the applicant. The request for information suspends the 60-day review period until the information is received. The suspension shall not exceed 30 days, unless justified by the nature of information requested or by exceptional circumstances;
  - **reject the application**. Prior to the rejection, the applicant can provide written comments within 30 days. Those shall be taken into account by the NCA of establishment when finalising the evaluation.

Mechanism to recognise services (3/13)

PUBLIC

Recognition of cloud computing service providers [Art. 17]

- NCAs of the other Member States have 60 days to review a draft recognition decision under Article 17.5 (a). Within the 60-day review period, NCAs may submit a **reasoned objection** and/or a **request for clarification:**
  - following a request for clarification, the NCA of establishment may ask **further information** from the applicant, confirm or modify its draft decision.
  - following a reasoned objection, the NCA of establishment shall **maintain or revoke its draft decision** and shall inform the other NCAs of its final decision within 15 days after the end of the 60-day review period;
  - in case of **continuous disagreement** between NCAs, the Commission shall, on the request of the concerned NCA, adopt a **binding decision** regarding the recognition of the applicant (implementing act).
- If there is **no reasoned objection** or **request for clarification**, the draft recognition decision is directly adopted and **the service is recognised** against the relevant UAL across the EU.
- The NCA of establishment may revoke its recognition decision if the CSP provided incorrect or misleading information.

Mechanism to recognise services (4/13)

PUBLIC

Conformity self-assessment [Art. 19]

- Cloud computing service providers **seeking recognition** in accordance with Article 17 for **UAL1**, need to **carry out a conformity self-assessment** of compliance with the criteria set out in Annex II.

- The cloud computing service provider needs to **issue an EU statement of conformity** and **make it publicly available**.

- By issuing such a statement, the cloud computing service provider **assumes responsibility** for the compliance of the service with the criteria for UAL1.

- Under Article 17(3), **for SME cloud computing service providers**, EU-issued conformity statements are **automatically accepted** in all Member States **without the need for prior recognition** under Article 17 by the evaluating national competent authority.

Mechanism to recognise services (5/13)

PUBLIC

Independent audit [Art. 20]

- Cloud computing service providers **seeking recognition** for **UAL 2-4** must undergo **at their own expense** independent **third-party audits** to obtain an **audit report** and an **audit opinion**

- Higher UALs must satisfy all the applicable cumulative criteria under Annex II. **Failure to meet any requirements of a lower UAL shall preclude conformity with the higher UAL**.

- **Audited providers** must cooperate with auditors, providing the necessary assistance, including by giving access to relevant data, premises, and information, and **must not obstruct** the audit.

- Auditing organisations shall ensure an **adequate level of confidentiality and professional secrecy** in respect of the information obtained from the audited providers and third parties as part of the audits

Mechanism to recognise services (6/13)

PUBLIC

Independent audit [Art. 20]

- Auditing organisations must be **independent, conflict-free, technically competent**, and **professionally objective**
- Audit **reports must document** the audit scope, methodology, findings, opinion (positive/negative), and, where applicable, recommendations or the recognised UAL
- If an audit cannot assess certain aspects, the report must **explain the reasons**.
- Auditors may **revoke** an audit report or opinion if the provider supplied false or misleading evidence.
- Audit reports and positive opinions must **be reviewed annually**, with auditors able to confirm, update, or revoke them.
- The Commission may adopt **detailed rules** on audit procedures, auditor requirements, methodologies, and report templates through delegated acts.

Mechanism to recognise services (7/13)

PUBLIC

Content and quality of audit evidence [Art. 21]

- To prepare the **audit report** and **audit opinion**, the auditing organisation shall assess the **compliance** of the audited service **with the criteria set out in Annex II** on the basis of the **audit evidence listed in Annex III**.

- The audit evidence shall be **relevant** and **sufficient** to enable the auditing organisation to prepare an audit report and audit opinion and **reliable**, according to the auditing organisation's professional judgment and scepticism.

Mechanism to recognise services (8/13)

PUBLIC

Central repository [Art. 22]

- The **Commission** shall establish and maintain a publicly available **repository of recognised cloud computing services**
- The **national competent authority of establishment** that recognised a cloud computing services, registers the service in the central repository
- The revocation of an audit report and audit opinion by an auditing organisation or the revocation of a recognition by a competent authority shall be published in the central repository and shall remain available there for five years
- The central repository shall be **regularly updated** by the Commission and the national competent authorities of establishment on a dedicated and easily accessible website.

Mechanism to recognise services (9/13)

PUBLIC

Transparency obligations [Art. 23]

- The recognised cloud computing service provider shall **notify** 1 – the auditing organisation and 2 – the NCA of establishment without delay, when becoming aware of **any information or material change** that may affect the audit report or the recognition.

- The auditing organisation shall assess whether the audit opinion or report needs to be amended or revoked. Where it amends or revokes the auditing opinion or report, it shall notify the NCA of establishment without delay.

- The NCA of establishment, on the basis of the notification of the cloud computing service provider or of the auditing organisation, shall assess whether the recognition needs to be amended or revoked. Where it amends or revokes the recognition, it shall notify the other NCAs and the Commission without delay.

Mechanism to recognise services (10/13)

PUBLIC

Penalties and compensation [Art. 24]

- Member States shall establish the **rules on penalties for infringements** of Chapter I, Title IV of CADA by cloud computing service providers subject to their competence.
- The penalties shall be **effective, proportionate and dissuasive**. Member States shall take into account the following non-exhaustive criteria for those penalties:
  - the nature, gravity, scale and duration of the infringement;
  - any remediation or mitigation action taken by the infringing party;
  - any previous infringement by the infringing party
  - the financial benefits or losses avoided for the infringing party due to the infringement;
  - any other aggravating or mitigating factor;
  - the infringing party's annual turnover in the preceding financial year in the Union.
- **Recipients** of the cloud computing service shall have the right to seek **compensation** from the cloud computing service providers for any damage or loss due to the infringement, in accordance with Union and national law.

Mechanism to recognise services (11/13)

PUBLIC

National competent authorities [Art. 25]

- Member States shall designate at least one **national competent authority** (NCA). They can **designate existing authorities** (recital suggests it could be data protection and/or cyber authorities)
- Member States shall notify the Commission of the NCA(s), and of their tasks and powers. The Commission will maintain a public register of NCAs.
- NCAs should perform their tasks in an impartial, transparent and timely manner, and benefit from adequate resources.
- The **Member State of establishment** has the exclusive competence for enforcing Chapter I, Title IV of CADA:
  - the main establishment of the service provider is defined as the **head office** or the **registered office** from which the principal financial functions and operational control are exercised.

Mechanism to recognise services (12/13)

PUBLIC

National competent authorities [Art. 26]

- In order to carry out their tasks related to the recognition of CSPs (Article 17), NCAs are granted with:
  - **investigative powers**, such as requesting for information and explanation, and carrying out or request inspections on premises;
  - **enforcement powers**, such as ordering the cessation of infringements, imposing fines, or imposing a periodic penalty payment.
- Measures taken by NCAs shall be effective, dissuasive and proportionate.
- Member States shall set out specific rules and procedures for the exercise of those powers.

Mechanism to recognise services (13/13)

PUBLIC

Mutual assistance and cross-border cooperation [Art. 27&28]

- NCAs and the Commission shall **cooperate closely** and provide each other with **mutual assistance**, including by **exchanging information**.
- A NCA of establishment can **request** other NCAs **to provide information or to exercise the powers of investigation:**
  - the NCA receiving the request can coordinate with other NCAs or public authorities within its Member State;
  - the NCA receiving the request shall comply and inform the NCA of establishment of any action taken within 2 months after receiving the request.
- NCAs, and the Commission, can ask the NCA of establishment to **re-assess the compliance** of a recognised CSP to the criteria for the relevant UAL, in case of doubt.
- Within 2 months, the NCA of establishment shall inform the requesting NCA, and the Commission, of its assessment and of any investigatory and enforcement measures taken or envisaged.

PUBLIC

A common approach to procure recognised service

Title IV: Procurement (1/4)

PUBLIC

Member States and Union entities risk assessments [Art.29]

- MS and Union entities must carry out **risk assessments** that:

(a) identify **public sector activities** that use or will make use of cloud computing services, that contribute to the **preservation of public order** in **Annex I or II** of the NIS2 Directive and in areas of **national security, internal security, external border management, defence, justice or law enforcement**, including the prevention, investigation, detection and prosecution of criminal offence;

(b) determine which **UAL (2-4) is appropriate** for the identified public sector activities.

- Where Union entities and Member States **share responsibilities**, they must consider carrying out the relevant risk assessment or assessments **jointly**.
- At least the following should be considered:
  - **sensitivity, criticality, and magnitude** of the **non-personal data processed** and the **nature, scope, context and purpose of processing of personal data**, as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects;
  - the **risk and consequent impact** of **unlawful access** under Union law to such data by a third country or a legal entity established in a third country;
  - the **risk and consequent impact** of possible **service disruption**

Title IV: Procurement (2/4)

PUBLIC

Member States and Union entities risk assessments [Art.29]

- The Commission must, by means of **implementing acts**, **specify the methodology** to be applied, the templates to be used and the elements to be considered for the risk assessments
- The methodology must specify **how MS use the highest UAL for the most critical public sectors activities including defence**
- Within **3 months** of carrying out the risk assessment(s) MS must provide the results to the Commission, indicating where they depart from the implementing acts specifying the methodology etc
- Through **implementing acts**, the Commission may set UALs for public sector activities where it concludes, based on a Member State's risk assessment, that the proposed UAL is inappropriate or does not sufficiently address public order concerns
- Where a risk assessment r**equires migration to another cloud computing service**, MS or Union entities must complete the migration within a **reasonable transition period, not exceeding 12 months**, while considering technical feasibility, service continuity, and data portability requirements
- Member States must **cooperate** with each other and the Commission, and the Commission may require cloud service providers to provide information necessary for risk assessments
- Consider whether a **multi-vendor or multi-cloud strategy** is appropriate in public procurement

Title IV: Procurement (3/4)

PUBLIC

Public procurement [Art.30]

- Article 30 applies to **contracting authorities that procure cloud computing services** for their exclusive use
- Contracting authorities (Union entities and public sector bodies) whose **activities have not been identified** under Article 29(1) **shall use UAL1** cloud computing services
- Contracting authorities whose a**ctivities have been identified** under Article 29(1) s**hall only procure UAL 2-4** cloud computing services
- Article 30(4) provides a **derogation** where contracting authorities may, **in duly justified exceptional cases, choose not to procure cloud computing services** with UALs 1–4 in one or more of the following circumstances:
  - **No suitable recognised service available** (and no reasonable alternative exists)
  - **Previous procurement failed** (no suitable tenders or participants received within the past year)
  - **Disproportionate cost** of complying with the Regulation

Title IV: Procurement (4/4)

PUBLIC

Impact assessments (Private sector entities) [Art.31]

- **Private sector entities** operating in sectors of high criticality **(Annex I of NIS2 Directive)** may carry out similar assessments as those set out in Article 29.
- The Commission **may issue guidance** on the methodology for carrying out those assessments and **possible mitigation measures**.
- The Commission **may adopt delegated acts to require private sector entities** operating in sectors of high criticality **to carry out those assessments and risk mitigation measures**, where necessary and in consultation with Member States.

PUBLIC

Thank you!

