Council of the European Union

Brussels, 30 October 2026
(OR. en)

14918/26

Interinstitutional File:
2026/0138 (COD)

LIMITE

TELECOM 502
CYBER 430
COMPET 1251
MI 1064
IA 274
CODEC 1982

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) - Presidency compromise text

INTRODUCTION

1. The Commission adopted the proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) on 4 June 2026[1].

2. The examination of the proposal in the WP Telecom started under the Cyprus Presidency on 16 June 2026. The Irish Presidency continued with the analysis of the text during four meetings of the WP Telecom on 7 July, 8 September, 22 September and 29 September, and it completed the first read-through of the entire proposal.

[1] Doc. 10104/26 + ADD 1.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

3. In addition, the Irish Presidency organised two online workshops on 21 September and 5 October, which allowed delegations, including capital-based experts, to raise specific questions and seek further clarifications directly from the Commission on the entire text of the proposal.

4. After the first online workshop, on 23 September, the Irish Presidency requested Member States to provide their initial drafting suggestions and written comments on Title IV (Autonomy) and Annexes II and III of the proposal. Title IV (Articles 16-44) and Annexes II and III correspond to Pillar 3 of the proposal.

5. Based on the input submitted by the Member States, the Irish Presidency has drafted the first, partial compromise text of the Cloud and AI Development Act proposal covering Pillar 3, which can be found in the Annex to this document. The Presidency has revised Articles 16-44, Annexes II and III, and some relevant recitals.

6. The Irish Presidency invites the delegations to discuss the changes proposed in this first partial compromise text during the WP Telecom meeting on 10 November 2026.

7. The changes in the document compared with the Commission proposal are marked as follows: additions are marked with **bold**, deletions are indicated with ~~strikethrough~~.

II. MAIN CHANGES

1. Chapter I, Section 1 – Union assurance levels (Articles 16-18)

1.1 The changes in **Article 16** clarify that the Union assurance levels recognition process is designed for specific services rather than providers. It has also been made clear that the review process, which is now referred in **paragraph 2**, would precede the adoption of delegated acts, and on the basis of technological developments, these acts would only amend some of the criteria for the Union assurance levels and not the levels themselves.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

1.2 **Article 17** has been redrafted to make the process of recognition of cloud computing services clearer, to eliminate repetitions, and to streamline the terminology used to describe the process. Notably, in **Article 17(3)** it is clarified that in the case of SMEs applying for Union assurance level 1, the evaluating competent authorities should register the EU statement of conformity in the central repository. **Point (b) in Article 17(5)** has been moved to the new **paragraph 5a** in **Article 17**, and another new **paragraph 7a** has been added to clarify that providers need to ensure continued compliance for services recognised at a specific Union assurance level. The modifications in **Article 17(9)** make it clear that competent authorities do not have to respond to reasoned objections individually, and the content of **paragraph 13** on the provision of information to the Commission has now been moved to **paragraph 10** of **Article 17**.

1.3 A new **Article 17a** has been added to describe in detail the process of revocation of recognition of a cloud computing service, which is referred to in **Article 17(11)**.

1.4 **Article 18** has been redrafted to provide more clarity on the process of identifying associated third countries. In particular, the second sentence in **point (c) of Article 18(1)** has been deleted because the policy objective is achieved with the first sentence of that point. The reference to implementing acts in **point (f)** has been moved to the new **Article 18(2c)**. Two **new paragraphs 2a and 2b** have been added to clarify the consequences of the Commission's revocation or suspension of the implementing act identifying a third country as associated, and to indicate that three or more Member States may request the Commission to review the associated status of a third country.

2. **Chapter I, Section 2 – conformity assessment procedures (Article 19)**

2.1 **Article 19** has been updated to ensure consistency with the redraft of **Article 17**.

2.2 A new **point 3a** has been added in **Article 19** to lay down a requirement for the Commission to publish a standard uniform template for the EU statement of conformity.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

3. **Chapter I, Section 3 – Independent third-party audits (Articles 20-24)**

3.1 The last sentence of **Article 20(1)** has been deleted to ensure clarity that each Union assurance level stands on its own and that providers do not need to complete the levels below if they wish their service to be recognised at levels 2-4. The last sentence in **Article 20(3)** on sharing information has been deleted because information sharing is now covered by the new **Articles 28a and 29b on professional secrecy and information sharing systems**. In **Article 20(4) point (a)** the 10-year period during which auditing organisations are expected not to have provided auditing services to the provider has been shortened to 5 years, in order to provide a more flexible framework for the rotation of auditors. In **Article 20(7)** it has been clarified that only substantial mistakes of providers should lead to the revocation of a positive opinion of an auditing organisation, and in **Article 20(8)** there is a modification of the requirement to submit the audit opinion for review – it would need to be done every two years instead of annually, to alleviate the burden for providers.

3.2 The last sentence in **Article 21(1)** has been deleted as it is a duplication with **Article 16**.

3.3 The deletion of the first sentence in **Article 22(3)** clarifies that audit reports and opinions should not be registered in the repository.

3.4 In **Article 23(1)**, a deadline of 7 days has been added for the provider to notify any material change in circumstances to the auditing organisation and the competent authority of establishment. The last sentence in **Article 23(3)** has been deleted because the revocation process is now covered by the new **Article 17a**.

3.5 In **Article 24 a new paragraph 2a** has been added to indicate the maximum ceilings for administrative fines that can be imposed for infringements of the provisions on the cloud computing sovereignty framework.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

4. **Chapter I, Section 4 – National competent authorities (Articles 25-26)**

4.1 In **Articles 25 and 26** (and throughout the text) the term 'national competent authorities' has been replaced with 'competent authorities', in line with existing legislation (e.g. the DSA).

5. **Chapter I, Section 5 – Mutual assistance and cooperation (Articles 27-28b)**

5.1 **Article 28** has been revised to clarify the mechanism for cross-border cooperation. In particular, in **paragraph 3** and the new **paragraph 3a**, further details have been added on the requests to the competent authority of establishment to assess compliance and take enforcement measures.

5.2 New **Articles 28a and 29b** have been added containing requirements to ensure professional secrecy and to use reliable and secure information sharing systems for all communications pursuant to the provisions on the cloud computing sovereignty framework.

6. **Chapter II, Section 1 – Public procurement (Articles 29-30)**

6.1 In **Article 29 (1) point (a)**, national security and defence have been deleted to clarify that these two areas would not be covered by the provisions on risk assessments. The wording in **point (a) of Article 29(2)** has been aligned with the wording of the annexes and the last sentence has been deleted as it is covered by the GDPR. In **Article 29(3)** a deadline has been introduced for the Commission to publish the risk assessment methodology and it has been clarified that the aim to the methodology is guidance for the Member States. The addition in **paragraph 4** clarifies that Member States' reporting obligations should follow the principles of necessity and data minimisation and must not create additional security exposure. **Article 29(5)** has been revised to remove the possibility for the Commission to adopt implementing acts on the Union assurance levels identified for the public sector activities by the Member States, replacing it with Commission recommendations, to which the Member States would be obliged to respond within 3 months. In **Article 29(6)** the period for the migration to another cloud computing service which may be mandated has been extended from 12 to 18 months.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

6.2 **Article 30 (1)** has been modified to extend the scope of the provisions on public procurement to contracting entities covered by Directive 2014/25/EU (private companies that procure under public procurement rules). Contracting entities are also included in the scope of the proposals for Chips Act 2 and the Industrial Accelerator Act, and these sectors are considered critical for public order (e.g. electricity and water supply). The text of the remaining paragraphs in **Article 30** has also been updated to align it with the wording of the proposals for Chips Act 2 and the Industrial Accelerator Act. Moreover, in **Article 30(2)** it has been clarified that public order criterion also applies to Union assurance level 1.

7. **Chapter II, Section 2 – Private sector entities (Article 31)**

7.1 In **Article 31 paragraph 3** has been deleted to clarify that there is no empowerment for the Commission to extend the scope to the private sector through a delegated act.

8. **Chapter II, Section 3 – Other procurement-related measures (Article 32-33)**

8.1 In **Article 32** the entire **paragraph 2** has been deleted because it largely reproduces requirements that already apply to award criteria under the existing EU public procurement framework. The content of this paragraph has been transferred to **Recital 67**, but without the content of **point (d)**, which concerns the requirement that Union Added Value criteria should not be "decisive" in the award of a contract, and which could create uncertainty in the context of existing public procurement rules.

8.2 In **Article 33**, the entire **paragraph 2** has been deleted because similar provisions on identifying barriers for SMEs in procurement procedures are included in the Public Procurement Directive. In **paragraph 3**, the frequency of Member States' reports to the Commission on their use of procurement of innovation in cloud computing services and AI systems has been reduced from annually to every three years, and in **paragraph 4** the exact percentage for the Member States to pursue as objective with regard to innovative SMEs and public procurement for cloud computing services and AI systems has been replaced with the phrase 'adequate percentage'. **Point (a) in Article 33(5)** has been deleted because preliminary market consultations is a horizontal requirement to be covered in the Public Procurement Act.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

9. **Chapter III – European public sector cloud federation (Articles 34-36)**

9.1 In **Article 34(3)** some further specifications for the platform for the EuroCloud Federation to be established by the Commission have been added. Moreover, it has been clarified in **Recital 69** that EuroCloud aims to bring together existing initiatives and that participation is voluntary.

9.2 **Article 35 (1)** has been revised to clarify the criteria the Commission will apply when assessing a sharing entity's control over an intermediate legal entity and to indicate that ownership is not a condition, but rather operational control. In **paragraph 2** it has been specified what measures the sharing entity should put in place to ensure an effective, secure and resilient provision of services, with the wording based on the NIS Directive. In paragraph 4, additional elements have been added on the need to inform the Commission of material changes and the possibility for the Commission to withdraw the authorisation to share services.

9.3 In **Article 36(1)** a clarification has been added on the characteristics of the fees to be charged by the Commission to the members of the EuroCloud Federation, based on the existing text of **Article 40**.

10. **Chapter IV – Procurement of data centre services, cloud computing services, software and AI systems by the Commission (Articles 37-40)**

10.1 In **Article 37(1)** AI models have been added to the list of items that the Commission may procure for itself and for Union entities and for contracting authorities of Member States. The modification in **Article 37(5)** is an alignment with the proposed amendment to **Article 38(10)**, so that both provisions consistently limit mandatory ancillary support to services that are objectively necessary for the procurement activity concerned. In **Article 37(6)** a reference to the interoperability of the common procurement platform has been added.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

10.2 In **Article 38**, **paragraph 2** has been deleted and its content has been included in **paragraph 1**. In **paragraph 3** it has been clarified that the division of responsibilities between the Commission and participating entities will be done in the agreement, and the last sentence on the Commission's responsibility for the operation and management of procurement activities has been moved to **paragraph 5**. In addition, **paragraph 5** also contains a sentence moved from **Article 39(4)** on the Commission's right to launch a procurement procedure open to participating entities without a prior specific request from them. In **paragraph 7** a safeguard has been included concerning the participation of a contracting authority of a Member State without that Member State's participation, and in **paragraph 8** a clarification has been made to ensure that smaller Member States are not discriminated with regard to access to procurement agreements.

10.3 In **Article 39(3)** a clarification has been made that a contracting authority that has acquired services and supplies from the Commission as a central purchasing body may offer those services and supplies to other contracting authorities without applying the public procurement procedures.

10.4 In **Article 40(5)** **point (d)** has been deleted as it is a duplication of **point (c)**. It has also been clarified which elements the Commission may take into account in the implementing act when setting the fees for participation in procurement activities.

11. **Chapter V – Open source (Articles 41-44)**

11.1 The title of **Article 41** has been updated to refer only to the promotion of open source solutions.

11.2 In **Article 43(1)** the term 'centralised' has been replaced with 'federated' as it describes more accurately the nature of the EU OSS Catalogue.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

12. **Annex II**

12.1 At the beginning of **Annex II**, a list of definitions has been added, so that the definitions of various terms that appear across the four assurance levels do not have to be repeated.

12.2 In **point 1.1 (c)** a cybersecurity derogation from the requirement for customer data to remain in the Union has been added. This has been replicated across levels 2 and 3.

12.3 In **points 1.1 (ga) and (gb)** the requirements for standards-based integration of external identity providers for authentication and access management and for the capability to record, retain, and review logs of management and data access activities have been added. This has been replicated across all levels.

12.4 In **point 2.1 subpoint (g) (iv)** has been deleted in line with changes in Article 18. Also, the scenario described in this subpoint is already covered by subpoint (iii). The same change has been made for level 3.

12.5 The modification in **point 2.1 (i)** clarifies that open source is not covered by the measures concerning software supply chain. The same change has been made for levels 3 and 4.

12.6 **Point 4.1 (j)** has been updated to expand the scope also to proprietary software.

13. **Annex III**

13.1 In the **first paragraph of Annex III** it has been clarified that the Annex is not exhaustive and that auditing organisations should take into account existing evidence for the purpose of the audits.

13.2 In **points 5 and 6 of criterion A** the references to payroll records, personnel timesheets, employment contracts and purchase orders have been removed.

13.3 In **criterion B** clarifications concerning location of infrastructure have been added in points **1(a) and 1 (ca)**.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

13.4 In **criterion C point 4** a reference to evidence demonstrating the audited organization has established a service agreement with each of its customers entities of the service has been added.

13.5 In **criterion E point 1** the changes are meant to ensure respect for data minimisation principle. In **point 3(b)** it has been clarified that a valid certificate should be issued under the national cybersecurity certification scheme in place in the Member State.

13.6 In **criterion G** additional requirements concerning the absence of third-country control or third-country entity control have been added in **points 1 and 2**.

13.7 Additional minor clarifications have been added in **criteria H-K**.

14. **Recitals**

14.1 **Recitals 37, 55, 59-64b, 67, 69, 71, 74, 76, 78-80, 84** have been aligned to reflect the changes in **Articles 16-44**. This includes new **Recitals 61a and 64b**.

14.2 The text deleted from **Recital 64** has been updated and added in the new **Recital 64a**.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act)

Recitals: 37, 55, 59-64b, 67, 69, 71, 74, 76, 78-80, 84

Articles: 16-44

Annexes II and III

RECITALS:

(37) Data centres are critical infrastructure for the Union, and can create substantial economic value, including valuable investments and jobs, and may support innovation ecosystems – especially if they are ~~integrated~~ **aligned** with local needs and follow best practices. If properly managed, the expansion of data centre capacity in the Union can bring significant economic and strategic benefits, help modernise the energy system, support clean energy growth and the sustainable use of energy. This depends on the implementation of an adequate framework preventing any negative impacts, such as energy supply stress, adverse environmental impacts and lost opportunities. Data centre acceleration zones ('acceleration zones') should contribute to this objective by enabling infrastructure deployment at scale and speed within a clear and streamlined regulatory framework.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(55) Independent audits are an important tool for monitoring the compliance of cloud ~~compuring~~ **computing** services provided by cloud computing service **providers**. Given the need to ensure that the applicable criteria for Union assurance levels 2, 3 or 4 are verified by third-party independent experts, cloud computing service providers should be accountable, through independent auditing, for their compliance with the criteria set out by this Regulation. Cloud computing service providers should be free to select the auditing organisation of their choice as long as the auditing organisation demonstrates the necessary independence and compliance with the requirements in this Regulation. To ensure that audits are carried out in an effective, efficient and timely manner, cloud computing service providers should provide the necessary cooperation and assistance to the organisations carrying out the audits, including by giving the auditing organisations access to all relevant data and premises necessary to perform the audit properly and answering oral or written questions. Auditing organisations should also be able to make use of other sources of objective information. Cloud computing service providers should not undermine the performance of the audit. Audits should be performed in accordance with best industry practices and high professional ethics and objectivity, with due regard for auditing standards and codes of practice. Auditing organisations should guarantee the confidentiality, security and integrity of the information, such as trade secrets, that they obtain when performing their tasks. That guarantee should not be a means to circumvent the applicability of audit obligations in this Regulation. Auditing organisations should have the necessary expertise in risk management and technical competence to audit cloud computing services. They should comply with core independence requirements for prohibited non-auditing services, firm rotation and non-contingent fees. If their independence or technical competence of auditing organisations is not beyond doubt, they should abstain or resign from the audit engagement.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(59) To ensure effective and consistent application of the cloud sovereignty framework, Member States should designate one or more competent authorities responsible for ~~recognising the auditing procedure and framework and the~~ **recognition of cloud computing services and** supervision of ~~recognised~~ cloud computing service providers**. This should be without prejudice to the possibility to designate one or more existing authorities, for example for specific sectors where existing authorities may be empowered, such as cybersecurity authorities, in accordance with national law**. Those authorities should be granted the necessary powers, resources, expertise and technical means to carry out their tasks in an effective, impartial and independent manner. Member States should ensure that the responsibilities of those authorities are clearly set out and that they cooperate closely with each other, with other relevant national authorities, including data protection authorities and cybersecurity authorities, and with the Commission, where appropriate, to ensure consistent supervision and facilitate the exchange of relevant information and best practices across the Union. ~~It should be possible for Member States to designate one or more existing authorities as competent authorities.~~

(60) The provision of mutual assistance between competent authorities is essential to ensure the effective supervision and enforcement of this Regulation across the Union borders, including through the timely exchange of information, coordination of investigative measures and support in the execution of tasks within the Union. Furthermore, effective enforcement requires robust cross-border cooperation between competent authorities to ensure the consistent application of this Regulation across Member States and the timely sharing of relevant information to address systemic risks within the Union

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(61) The Union's objective of strengthening its autonomy should be pursued in a manner that remains open, cooperative and consistent with the Union's international commitments and partnerships. The policy objectives pursued through Union assurance levels 1, 2, and 3 should therefore be understood as the Union's capacity to act autonomously where necessary, while remaining engaged with its international partners and fostering mutually beneficial cooperation. Against this background, the Commission may decide, for Union assurance level 3, that a cloud computing service **provider** subject to the control of a third country or a legal entity established in a ~~third country~~ **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. **To verify that a third country has implemented the necessary safeguards,** the Commission should assess whether the third country is covered by an adequacy decision adopted pursuant to Article 45 of Regulation (EU) 2016/679~~. In particular, it should be determined~~ **and** whether the adequacy decision applies ~~generally~~ to the third country as a whole or is limited to specific sectors or certified organisations. It should be further assessed whether the scope of the adequacy decision extends to the specific processing activities that are carried out in the context of the service provision, or whether transfers remain subject to the requirements to implement appropriate safeguards. **In addition, to ensure that data held in the Union is protected against third country government access or transfer, the Commission should asses whether the legal system and practices of the third country do not enable that third country to access or transfer non-personal data held in the Union by a cloud computing service provider in a manner that is contrary to Article 32 of Regulation (EU) 2023/2854.**

(61a) When assessing the equivalent levels of access to public procurement procedures for cloud computing services the Commission should take into account both the legal framework and any potential technical or structural barriers to public procurement procedures.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(62) To ensure a coherent and risk-based approach to the autonomy of the Union, Member States and the Union entities should carry out one or more risk assessments to determine ~~public-sector~~ **public sector** activities that ~~concerns~~ **concern** public order. The risk assessment should determine which Union assurance level is appropriate for the **public sector** activities~~, due to~~**.** **In carrying out** their ~~importance in preserving public order in sectors falling under~~ **risk assessments, Member States and Union entities should consider existing sectoral and horizontal risk-management frameworks, including those established pursuant to** Directive (EU) 2022/2555 and ~~in the areas of~~ national ~~security, internal security, external border management, defence, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal offence~~ **cybersecurity legislation, with the objective of avoiding duplication of assessments, overlapping compliance obligations and unnecessary administrative burdens**. To ensure consistent application of this Regulation and preserve the integrity of the digital single market, the Commission will provide ~~guidance~~ **a methodology** to assist Member States in carrying out their risk assessments. Whereas the determination of the level of sensitivity of information that may be hosted in a cloud computing service that offers a Union assurance level lies within the competence and discretion of the Member States, to provide consistency across the Union, Union assurance levels 3 and 4 should allow for the secure hosting of EU classified information.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(63) In their risk assessments, Union entities and Member State shall assess the sensitivity, criticality**, and volume** ~~and magnitude~~ of personal **data** and non-personal data **stored or** processed ~~in cloud environment~~ **including the potential impact on public order, as well as the nature, scope, context and purpose of processing of personal data**. Such processing may include ordinary business information, commercially sensitive information, operationally critical data, personal data within the meaning of Regulation (EU) 2016/679, and data that is subject to sector-specific obligations under Union law, including Directive (EU) 2022/2555 and Regulation (EU) 2022/2554. ~~The guidance by the Commission allows for a degree of flexibility to Union entities and Member States in determining the appropriate Union assurance levels and the categories of information and users for which such levels are appropriate. At the same time,~~ Divergent national approaches to the classification and mapping of data sensitivity and assurance requirements may undermine the consistent application of the sovereignty framework across the Union. To ensure harmonised implementation across the Union, the Commission should, in cooperation with relevant authorities, provide ~~centrally coordinated guidance~~ **a methodology to guide the Member States and Union entities** on the mapping between Union assurance levels and **the public sector activities, taking into account the** categories of information, ~~taking into account~~ the sensitivity, criticality and ~~magnitude~~ **the volume** of the data processed ~~by the cloud environment, the systematic~~**, the systemic** importance of the activities of the contracting authorities, and the applicable obligations arising from Union law. **In developing the methodology, the Commission should allow for a degree of flexibility to Union entities and Member States in determining the appropriate Union assurance levels and the categories of information and users for which such levels are appropriate.** Furthermore, the criteria under the Union assurance levels should not affect obligations of cross-border cooperation provided by Union law. Where cloud computing services are used to process personal data, Regulation (EU) 2016/679 provides for an obligation to agree on organisational and technical measures to comply with that Regulation. Where the cloud computing service provider relies on subcontractors in the provision of the services, the same agreements apply to the subcontractors. Where specific technical and organisational measures should be implemented pursuant to this Regulation to ensure that personal data are processed in line with this Regulation, such specific measures could be foreseen in the mandatory agreements pursuant to Regulation (EU) 2016/679 and could be relied on to demonstrate that the necessary Union assurance levels are met.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(64) The free flow of data within the Union is an essential condition for the proper functioning of the internal market. To promote the free flow of data within the Union and to support the functioning of the internal market, it is appropriate that Member States ensure that data is not confined to the territory of a single Member State and may be stored and processed across the Union without unjustified restrictions ~~restrictions. The Union maintains an open and non-discriminatory framework for market access, in accordance with the TFEU and subject to international commitments. Those include commitments under the World Trade Organization (WTO) Agreement on Government Procurement (GPA), as well as bilateral trade agreements. Nevertheless, where necessary and in duly justified circumstances, the Union retains the right, in accordance with Article III:2(a) of the WTO GPA, to adopt or maintain measures necessary to protect public morals, order or safety, allowing for necessary and proportionate restrictions on access to public procurement procedures. Indeed, identifying and addressing risks such as critical dependencies, unauthorised access to Union data, technology leakage, sabotage and espionage by third-country actors is fundamental for preserving Union public order. Preserving the protection of public order of the Union and its Member States requires a prudent but firm political, legal and operational response for both national and Union-level award procedures, in full respect of international commitments. To protect and preserve the public order of the Union and its Member States, contracting authorities whose activities have been identified on the basis of the Member State risk assessment should therefore procure only the cloud computing service providing the appropriate level of assurance between levels 2 and 4. A minimum assurance level, by mandating Union assurance level 1 across the Union, is necessary to establish a consistent baseline of safeguards for the public sector, thereby reducing vulnerabilities in the public sector to third country access to Union data and disruption of services.~~.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(64a) The Union maintains an open and non-discriminatory framework for market access, in accordance with the TFEU and subject to international commitments. Those include commitments under the World Trade Organization (WTO) Agreement on Government Procurement (GPA), as well as bilateral trade agreements. Nevertheless, where necessary and in duly justified circumstances, the Union retains the right, in accordance with Article III:2(a) of the WTO GPA, to adopt or maintain measures necessary to protect public morals, order or safety, allowing for necessary and proportionate restrictions on access to public procurement procedures. Identifying and addressing risks such as critical dependencies, unauthorised access to Union data, technology leakage, sabotage and espionage by third-country actors is fundamental for preserving Union public order. Preserving the protection of public order of the Union and its Member States requires a prudent but firm political, legal, and operational response for both national and Union-level procurement procedures, in full respect of international commitments. To protect and preserve the public order of the Union and its Member States, Union entities, contracting authorities, and contracting entities should at least procure, as a baseline, cloud computing services recognised at a Union assurance level 1. Mandating a minimum assurance level is necessary and proportionate to address and mitigate those risks, such as critical dependencies, unauthorised access to Union data, technology leakage, sabotage and espionage by third-country actors, facing the public sector as a whole. For public sector activities identified in the risk assessments, Union entities, contracting authorities and contracting entities should procure Union assurance level 2, 3, or 4.

(64b) On an exceptional basis and where duly justified, Union entities, contracting authorities and contracting entities should be able to derogate from procuring specific Union assurance levels where justified. With regard to disproportionate costs, these could include estimated cost differences exceeding 25%, based on objective and transparent data.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(67) In public procurement procedures for cloud computing services and AI systems, contracting authorities **and Union entities** should include ~~clear European~~ **criteria to measure the tender's** added value **for the Union** as part of ~~the quality~~ **its** evaluation ~~of the tender~~. Such **Union** added value should consist in helping reinforce the digital supply chain in the Union; integrating Union technologies; conducting the innovation required to deliver the service in the Union; and delivering the service using hardware components designed or manufactured in the Union. **Union entities and contracting authorities applying the Union** ~~The criterion relating to European~~ added value **criteria** should ~~not be decisive for award~~ **ensure that such criteria comply with Union public procurement rules, including ensuring that the use is linked to the subject matter** of the contract ~~and should be applied in a manner that preserves the primacy of technical and financial criteria directly connected to the performance requirements~~**, do not confer unrestricted freedom of choice on the contracting authority, and are expressly set out in the procurement documents or in the contract notice**. For this purpose, contracting authorities could consider a maximum weighting of 15 out of 120 points to be allocated to ~~European~~ **Union** added value within the overall evaluation methodology, ensuring that it remains proportionate and subordinate to the core contract award criteria.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(69) In the joint declarations 'Building the next-generation cloud for businesses and the public sector in the EU' of 15 October 2020 ([1]) and the Berlin Declaration on Digital Society and Value-Based Digital Government of 8 December 2020 ([2]), Member States expressed great interest in determining a common approach to federating cloud capacities by interconnecting cloud computing infrastructures across the Union and working towards the deployment of a secure and interoperable European public-sector cloud federation. In its conclusions on the future of EU digital policy of 21 May 2024 ([3]), the Council of the European Union confirmed the relevance and importance of achieving this common approach by inviting the Commission to continue its support for the development of interoperable public digital services and the cross-border interconnection of public administrations' infrastructure, including cloud and edge infrastructures, to increase their resilience, efficiency and sustainability. To achieve this common approach, it is necessary to establish the European public-sector cloud federation ('the EuroCloud Federation'). The EuroCloud Federation should bring together **existing** national and European cloud initiatives that provide highly trusted and secure public-sector cloud capabilities and facilitate the sharing of such **existing** capabilities between Union entities and public-sector bodies**. Participation in the EuroCloud Federation is entirely voluntary and its members retain full discretion to determine whether to share or use services and if so, which services to share or use within the EuroCloud Federation**. When evaluating this Regulation, the Commission may, at a later stage, assess the possibility for acceding countries, candidate countries and potential candidates, as well as for international organisations whose headquarters are in the Union, to participate in the EuroCloud Federation, in accordance with Union law.

Agence Europe

1 Joint declaration, 'Building the next generation cloud for businesses and the public sector in the EU', 15.10.2020, https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.

2 Berlin Declaration on Digital Society and Value-based Digital Government, 8.12.2020, https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government.

3 Council conclusions on the Future of EU Digital Policy, 21.5.2024, https://data.consilium.europa.eu/doc/document/ST-9957-2024-INIT/en/pdf.

Obtenu pour vous par
Obtained by
agence europe

(71) Participation within the EuroCloud Federation should be limited to public entities, without direct participation of a private party. In this regard, direct private participation should be excluded where the sharing entity, either directly or indirectly through an intermediate legal entity, ~~owns the hardware, as defined in Article 3, point (5), of Regulation (EU) 2024/2847 of the European Parliament and of the Council ([4]), over~~ **operates the physical assets through** which the service is made available, and provides that service. The sharing entity should be deemed to exercise control over that intermediate legal entity where the following cumulative conditions are fulfilled. First, the sharing entity should exercise a decisive influence over both **the** strategic objectives and significant decisions of the intermediate legal entity that ~~owns the hardware~~ **operates the physical assets** and provides the ~~services~~ **service**. Second, there should not be any direct private capital participation in that intermediate legal entity. Third, more than 80% of the activities of the intermediate legal entity should be carried out in the performance of tasks entrusted to it by the sharing entity.

Agence Europe

[4] ~~Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).~~

Obtenu pour vous par
Obtained by
agence europe

(74) Contracting authorities of Member States frequently encounter significant difficulties in procuring digital solutions such as data centre services, cloud computing services, software ~~and~~**,** AI systems **and AI models**. Limited financial resources, reduced purchasing power, insufficient technical or procurement expertise prevent public-sector bodies from effectively accessing such services. Procurement activities conducted by the Commission in concertation with the contracting authorities of Member States can play a decisive role in harnessing collective purchasing power and ensuring access to those services and supplies on favourable terms. The Commission may already carry out joint procurement procedures with contracting authorities of Member States pursuant to Article 168(2) of Regulation (EU, Euratom) 2024/2509. The Commission may also already act as a wholesaler by ~~buiying~~ **buying**, stocking, and reselling or donating supplies and services to partner organisations selected by it. In order to enable those entities to fully exploit the potential of the internal market, in particular as regards economies of scale and benefit sharing, the possibilities for the Commission to act as a central purchasing body should be extended to contracting authorities of Member States and to partner organisations selected by the Commission, as a form of procurement additional to those in Article 168(3) of the Regulation (EU, Euratom) 2024/2509. It should be possible for the Commission to use all the procurement procedures available for the benefit of contracting authorities of Member States and of partner organisations selected by the Commission and to include purchasing activities conducted by the Commission for Union institutions, bodies and agencies. Contracting authorities of Member States, partner organisations and Union institutions, agencies and bodies should be considered as 'participating entities' in those procurement procedures. **Participation in procurement activities should remain voluntary and should be without prejudice to the ability to conduct public procurement procedures independently in accordance with Union law.**

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(76) The Commission should present to the Member States a draft agreement setting out the practical arrangements governing the procurement activities. Given the potentially large number of participating entities involved, that draft agreement should be negotiated and initially concluded between the Commission and the Member States willing to participate. It should lay down the conditions and procedure by which Union entities as well as other Member States, contracting authorities of Member States and partner organisations selected by the Commission may subsequently accede to and benefit from it**, including conditions and time frames for possible opt-in and opt-out and those related to the responsibilities of the Commission and participating entities. Accession to the agreement, and subsequent participation in framework contracts or dynamic purchasing systems should not create any obligation to award or enter into specific contracts under the relevant procedure, nor should it give rise to any financial commitment prior to entering into specific contracts**. The agreement will enter into force in accordance with its provisions, subject to the approval of at least two Member States. Although the Commission should, as far as possible, aim to address the common needs of participating entities, this should not be construed as an obligation to satisfy needs that are specific to a limited number of them.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(78) The agreement should establish a Steering Committee composed of the Commission and representatives of Member States. The **Steering** Committee ~~is~~ **should be** responsible for strategic oversight of the procurement activities, including the strategic guidance of the agenda of public procurement activities ~~and of each procurement procedure~~. The Steering Committee should also oversee the involvement of participating entities**, and should set the conditions for contracting authorities of Member States to accede to the agreement. Contracting authorities should be allowed to accede to the agreement and participate in the procurement activities carried out by the Commission even if their respective Member State is not party to the agreement, provided that such participation is not contrary to applicable national law. The contracting authorities should be solely responsible for ensuring compliance with the law of their Member State and the Commission should not be responsible for verifying whether such participation does not conflict with applicable national law**. The Steering Committee should not be responsible for the operations of procurement activities, which should remain the responsibility of the Commission, including the setting of fees. The Steering Committee should provide for the most adequate method to select additional representatives from Union entities, from contracting authorities from Member States and from partner organisations selected by the Commission.

(79) The rules governing responsibility and the applicable public procurement framework between the Commission, acting as a central purchasing body, and the participating entities procuring through it should be clarified in the agreement. Where a participating entity conducts certain parts of the procurement procedure autonomously, it should remain solely responsible for ~~those~~ **the** stages of autonomous conduct**, such as awarding contracts**. A contracting authority which acts as a central purchasing body and has acquired services or supplies through the Commission should be permitted to offer those services to other contracting authorities without applying the public procurement procedures provided for under applicable Union law. In that case, the contracting authority is bound to comply with the initial contractual provisions in any subsequent contract.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(80) In order to ensure that the necessary resources remain available, the participating entities ~~will~~ **should** contribute to the costs incurred in the procurement procedures and any ancillary activity. To this end, the Commission should be entitled to charge fees to the participating entities. Those fees should be set at a level sufficient in principle to cover all the direct and indirect costs incurred by the Commission in connection with the procurement activities, including any ancillary services. Those fees should be established in accordance with practices of comparable procurement frameworks. **For the purpose of determining the fees, the Commission should take into account relevant parameters such as, but not limited to, the volume of services and supplies to be consumed, the commitment to use a specific minimum volume of supplies or services over a given period, and the maximum amount payable for the services or supplies concerned as specified in the applicable arrangements.** Initial establishment costs may be borne by the general budget of the Union and reimbursed by the participating entities over a set period. Revenues generated by the fees should constitute internal assigned revenues within the meaning of Article 21(3)(a), of the Regulation (EU, Euratom) 2024/2509.

(84) In order to ensure effective and consistent implementation across the Union of the obligations to conduct an open-source assessment and to make software available for reuse, it is necessary to set up a network of open-source programme offices ('the OSPO network')**, building on the existing initiatives,** bringing together**, on a voluntary basis,** the relevant structures within Union entities and Member States. This OSPO network should promote coordination between open-source programme offices established at local, regional or national level and by Union entities. The OSPO network should facilitate the exchange of information and best practices.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

ARTICLES:

TITLE IV
AUTONOMY

Chapter I
Cloud computing sovereignty framework

SECTION 1
UNION ASSURANCE LEVELS

Article 16

Scope

1. This Chapter establishes a Union cloud computing sovereignty framework comprising four Union assurance levels, the criteria for which are set out in Annex II, that cloud computing service providers **and their cloud computing services** shall meet in order to provide their cloud computing services to Union entities and public sector bodies.

2. **To ensure Annex II and Annex III remain up to date with new legal or technical developments,** the Commission ~~is empowered to adopt delegated acts in accordance with Article 45 to amend the Union assurance levels set out in Annex II and the evidence set out in Annex III~~ **shall review them at least every 18 months**.

3. ~~To ensure Annex II and Annex III remain up to date with new legal or technical developments~~ **On the basis of the review referred to in paragraph 2**, the Commission ~~shall review them at least every 18 months~~ **is empowered to adopt delegated acts in accordance with Article 45 to amend the criteria for the Union assurance levels set out in Annex II and the evidence set out in Annex III, with the exception of the criteria in Annex II concerning establishment, control by a third country, location and personnel, and with the exception of point 11 of Annex III**.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

Article 17

Recognition of cloud computing ~~service providers~~ services

1. **Where** a cloud computing service provider ~~that aims to be~~ **intends to have a cloud computing service** recognised ~~as offering~~ **at** a Union assurance level, **it** shall submit an application for recognition to the ~~national~~ competent authority of establishment~~. When submitting an application for recognition, the cloud computing service provider shall include all the relevant evidence required under paragraphs 3 or 4.~~ **('the evaluating competent authority').**

2. ~~The competent authority of establishment shall be~~ The evaluating ~~national competent authority. An evaluating national~~ competent authority that has received an application for ~~a candidate~~ recognition~~,~~ may, where **it deems collaboration** necessary, request ~~one or more~~ **other** competent authorities ~~of the other Member States~~ to collaborate in the ~~procedure for a candidate~~ recognition ~~under this Article~~ **procedure**. Within 15 days of receiving ~~such a request, the national authority that has received~~ a request for collaboration ~~shall either provide confirmation that it agrees to collaborate with the evaluating national~~**, the** competent authority **shall either confirm collaboration in the recognition procedure or decline** ~~or refuse~~ the request.

3. ~~For~~ **Where a cloud computing service provider intends to have a cloud computing service recognised at** Union assurance level 1, the ~~candidate~~ cloud computing service provider shall submit ~~to the evaluating national competent authority~~ the EU statement of conformity ~~referred to in~~ **issued under** Article 19(2) and all the **evidence** necessary ~~evidence~~ **for the evaluating competent authority to assess the application for recognition**.

   By way of derogation from the first ~~subparagraph~~ **subparagraph**, **where the cloud computing service provider which issued** the EU statement of conformity ~~issued under Article 19(2) by~~ **is an SME, it shall submit the EU statement of conformity to the evaluating competent authority, which shall register, without delay, the concerned** cloud computing service ~~providers that are SMEs~~ **in the central repository. Upon registration in the central repository, the cloud computing service** shall be directly and automatically recognised ~~in all Member States~~ **at Union assurance level 1 across the Union** without the need for ~~prior~~ **a** recognition **decision** by the evaluating ~~national~~ competent authority.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

4. ~~For~~ **Where a cloud computing service provider intends to have a cloud computing service recognised at** Union assurance levels 2, 3 ~~and 4, the candidate~~ **or 4, the** cloud computing service provider shall submit to the evaluating ~~national~~ competent authority the audit report, the 'positive' audit opinion ~~referred to in Article 20~~**,** and all the **audit** evidence provided to the auditing organisation ~~during the audit procedure~~.

5. Within 60 days of ~~accepting an~~ **receiving a complete** application pursuant to paragraph 1, the evaluating ~~national~~ competent authority shall assess the **application and** evidence submitted ~~pursuant to paragraphs 3 or 4~~ and shall either:

   (a) prepare a draft recognition decision and notify, as soon as possible, the competent authorities of the other Member States for a 60-day review period to confirm its intended recognition of the cloud computing service across the Union as offering the applicable Union assurance level. The notification to the competent authorities of the other Member States of the review period shall include the evidence referred to in paragraphs 3 or 4; or

   (b) ~~where the evidence submitted is insufficient to allow the evaluating competent authority to recognise the cloud computing service, it may request further information from the applicant and request that the applicant submit such information within a specified time limit. The period of 60 days referred to in this paragraph shall be suspended from the date of issue of the request until the date the information is received. The suspension shall not exceed 30 days in total unless it is justified by the nature of the information requested or by exceptional circumstances;~~

   ~~or~~

   (c) reject the ~~request~~ **application** for recognition **where it considers the cloud computing service does not fulfil the criteria of the appropriate Union assurance level**. Prior to rejecting the request for recognition, the evaluating competent authority shall give the ~~candidate~~ cloud computing service provider the opportunity to provide written comments ~~on the conclusions of the evaluation~~ within 30 days. **Taking due account of those comments,** the evaluating competent authority shall ~~take due account of those comments when finalising its conclusions~~ **either reject the application or prepare a draft recognition decision in accordance with paragraph 5, point (a)**.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

5a. Where the evidence submitted is insufficient to allow the evaluating competent authority to asses the application, it may request the cloud computing provider to provide any additional relevant information within a specified time limit. The period of 60 days referred to in the first subparagraph of paragraph 5 shall be suspended from the date of the request until the date the information is received. The suspension shall not exceed 30 days in total unless it is justified by the nature of the information requested or by exceptional circumstances.

6. During the review period referred to in paragraph 5, point (a), the national competent authority of another Member State may submit a reasoned objection or request for clarification to the evaluating national competent authority, where it considers that the draft recognition decision does not comply with the applicable Union assurance level set out in Annex II.

7. Where no reasoned objection or request for clarification is submitted within the review period referred to in paragraph 5, point (a), the ~~conclusions by the evaluating national competent authority~~ **draft recognition decision** shall be deemed accepted by ~~all Member States,~~ **the other competent authorities.** The evaluating ~~national~~ competent authority shall adopt the recognition decision and the ~~audited~~ **cloud computing** service shall be recognised throughout the Union at the appropriate Union assurance level **without any additional national requirements**.

7a. Where a cloud computing service has been recognised at a Union assurance level, the cloud computing service provider shall ensure continuous compliance with the criteria set out in Annex II for the respective Union assurance level.

8. Where a request for clarification is submitted within the review period referred to in paragraph 5, point (a), the evaluating ~~national~~ competent authority shall take due account of such request and, where applicable, request new information from the ~~applicant as per~~ **cloud computing service provider under** paragraph ~~5, point (b) or confirm~~**5a, maintain** or modify its original draft **recognition** decision. Where ~~the requesting~~ **a** competent authority ~~is not satisfied~~ **that submitted a request for clarification under paragraph 6 continues to disagree with the draft recognition decision**, it may submit a reasoned objection.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

9. Where a reasoned objection is submitted within the review period referred to in paragraph 5, point (a), ~~or following the procedure referred to in paragraph 8,~~ the evaluating ~~national~~ competent authority shall assess the objection and shall either maintain ~~or revoke its original~~ **its** draft **recognition** decision **or reject the application in accordance with paragraph 5 (c)**. **Where more than one competent authority submit a reasoned objection,** the evaluating ~~national~~ **competent authority may assess them jointly. Within 15 days after the end of the review period referred to in paragraph 5, point (a), the evaluating** competent authority shall inform the competent authorities of the other Member States ~~within 15 days after the end of the review perioed referred to in paragraph 5, point (a), or within 15 days after receiving~~ **about the assessment of** the reasoned ~~objection following the procedure referred to in paragraph 8, whichever is applicable~~ **objections and whether it intends to maintain its draft recognition decision**.

10. ~~In case~~ **Where** the evaluating ~~national~~ competent authority intends to maintain its draft **recognition** decision, ~~the concerned national~~ **any** competent authority **that submitted a reasoned objection** may refer the matter to the Commission. The Commission shall assess the referral and may request ~~information from~~ the **evaluating** national **authority or the** competent authorities ~~concerned~~ **that submitted a reasoned objection to provide without delay any relevant information concerning the application for recognition**. The Commission shall **within a reasonable period** adopt a binding decision determining whether the evaluating ~~national~~ competent authority may adopt the recognition decision.

11. The evaluating ~~national~~ competent authority may revoke its recognition **in accordance with Article 17a** where it finds that a cloud computing service provider~~, whose service was recognised across the Union as providing a specific Union assurance level,~~ intentionally or negligently, supplied incorrect or misleading information.

12. The Commission may adopt implementing acts concerning the practical arrangements for the procedures referred to in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

13. ~~The Commission may, in order to carry out the tasks assigned to it under paragraph 10 , require that national competent authorities of establishment provide, as soon as possible and within a reasonable period, any relevant information relating to the concerned cloud computing service provider and the application for recognition.~~

14. When sending a request for information, **the evaluating competent authority or** the Commission shall state the purpose of the request, specify what information is required and set the period within which the information is to be provided.

Article 17a

Revocation of recognition

1. Where the evaluating competent authority intends to revoke the recognition of a cloud computing service, it shall notify without delay the competent authorities of the other Member States. The evaluating competent authority shall provide a summary of the facts and conclusions that support the revocation of the recognition.

2. Where a competent authority request clarification, the evaluating competent authority shall without delay provide the necessary information and assistance.

3. Within 30 days of receiving the notification referred to in paragraph 1, a competent authority may submit a reasoned objection if it disagrees with the revocation of the recognition.

4. Where, following a reasoned objection, the evaluating competent authority intends to maintain its draft revocation decision, any competent authority that submitted a reasoned objection may refer the matter to the Commission. The Commission shall assess the referral and may request any necessary information from the evaluating competent authority or from any competent authority that submitted a reasoned objection. The Commission shall adopt a binding decision determining whether the evaluating competent authority may revoke its recognition.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

5. Before revoking a recognition decision, the competent authority of establishment shall give the concerned cloud computing service provider the opportunity to provide, within 15 days, written comments.

6. Where the evaluating competent authority revokes the recognition of a cloud computing service, it shall notify without delay the competent authorities of the other Member States.

The evaluating competent authority shall provide in its revocation decision for a sufficient transition period of at least 12 months before the revocation becomes applicable.

Article 18

Associated third countries

1. **For the purpose of recognising at Union assurance level 3 a cloud computing service provided by a cloud computing service provider subject to the control of an associated third country or a legal entity established in an associated third country,** the Commission may adopt decisions, by means of implementing acts, identifying third countries ~~for which cloud computing service providers subject to the control of that third country or a legal entity established in that third country may be audited against the criteria for Union assurance level 3 pursuant to Annex II, provided that that third country fulfils~~ **as associated if** the following cumulative criteria **are fulfilled**:

   (a) ~~it~~ **the third country** is subject to a relevant adequacy decision adopted under Article 45 of Regulation (EU) 2016/679;

   (b) ~~it has no measures in place that~~ **the legal system and practice of the third country do not** enable ~~it to exercise control over the~~ **that third country to access or transfer non-personal data held in the Union by** cloud computing service ~~provider in a way that would conflict with the requirements for lawful access to non-personal data set out in paragraphs 2 and 3 of~~ **providers in a manner that is contrary to** Article 32 of Regulation (EU) 2023/2854;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(c) ~~it~~ **the third country** has no measures in place to compel ~~the~~ cloud computing service ~~provider~~ **providers** to degrade or disrupt service continuity or provision~~. It also has no measures in place to oblige the cloud computing service provider to implement, enforce, give effect to, or comply with 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) ~~it~~ **the third country** has no measures in place to impede the provision of state-of-the-art technologies and services provided by ~~the~~ cloud computing service ~~provider~~ **providers**;

(e) ~~it~~ **the third country** maintains an open market to ~~Union~~ cloud computing ~~services~~ **service providers subject to the control of a Member State or of a legal entity established in the Union**;

(f) the third country grants equivalent levels of access to public procurement procedures ~~of~~ **for** cloud computing services **provided by cloud computing service providers** subject to the control of a ~~Union~~ Member State ~~or entity~~ or a legal entity established in the Union.

~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2)~~

2. Where available information reveals that ~~the~~ **an associated** third country no longer fulfils the requirements under paragraph 1, the Commission shall**, by means of implementing acts,** repeal~~, amend~~ or suspend the decision referred to in paragraph 1. **The Commission shall notify without delay the competent authorities. The implementing acts referred to in this paragraph shall not be immediately applicable and shall lay down appropriate transition periods and measures.**

2a. Where the Commission repeals or suspends the decision referred to in paragraph 1, the competent authority of establishment shall suspend or revoke, in accordance with Article 17a, the recognition decisions at Union assurance level 3 for services provided by cloud computing service providers subject to the control of that third country or a legal entity established in that third country.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

2b. Where available information reveals that an associated third country may no longer fulfil the requirements under paragraph 1, three or more Member States may request the Commission to review the associated status of a third country. Upon a duly substantiated request, the Commission shall assess the request within three months of its submission and, where appropriate, revoke or suspend the implementing act identifying that third country as associated in accordance with paragraph 2.

2c. The implementing acts referred to in paragraphs 1 and 2 shall be adopted in accordance with the examination procedure referred to in Article 46(2).

3. The Commission shall publish on its website a list of **associated** third countries ~~that fulfil the requirements~~ **identified** under paragraph 1 and ~~those that~~ **third countries** no longer ~~do so~~ **identified as associated following the suspension or revocation of the decision under paragraph 2**.

SECTION 2

CONFORMITY ASSESSMENT PROCEDURES

Article 19

EU statement of conformity ~~self-assessment~~

1. **Where a** cloud computing service ~~providers seeking recognition in accordance with Article 17 as offering~~ **provider intends to have a cloud computing service recognised at** Union assurance level 1, **it** shall carry out a conformity self-assessment ~~of~~ **to demonstrate** compliance with the criteria for Union assurance level 1 set out in Annex II.

2. Following the self-assessment referred to in paragraph 1, the cloud computing service provider shall issue an EU statement of conformity stating that **the cloud computing service is in** compliance with the criteria for Union assurance level 1 ~~have been demonstrated~~. By issuing ~~such~~ a statement **of conformity**, the cloud computing service provider ~~shall assume~~ **assumes** responsibility for the compliance of the cloud computing service with the criteria for Union assurance level ~~1set out in Annex II~~**1**.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

3. The cloud computing service provider shall make the EU statement of conformity publicly available.

3a. The Commission shall publish a standard uniform template for the EU statement of conformity and make it available in a digital format in all official languages of the Union.

SECTION 3

INDEPENDENT THIRD-PARTY AUDITS

Article 20

Independent audit

1. Cloud computing service providers seeking recognition ~~in accordance with Article 17 as offering~~ **of a cloud computing service at** Union assurance level 2, 3, or 4 **('audited provider')**, shall undergo at their own expense, independent third-party audits to obtain an audit report and an audit opinion from an auditing organisation. ~~An audited provider undergoing an audit procedure at a higher Union assurance level shall satisfy all the applicable cumulative criteria under Annex II applicable to the lower Union assurance levels. Failure to meet any requirements of a lower assurance level shall preclude conformity with the higher Union assurance levels.~~

2. Audited providers shall cooperate with auditing organisations and provide them ~~assistance~~ **with the** necessary **assistance** to enable them to conduct those audits in an effective, efficient and timely manner, including by giving them access to all relevant data and premises and by answering oral or written questions. Audited providers shall refrain from hampering, unduly influencing or undermining the performance of the audit.

3. 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, including after the audits have ended. That requirement shall not adversely affect the performance of the audits and other provisions of this Regulation. ~~Under Article 23, the auditing organisation shall only share information that are necessary for the reporting purposes and do not contain any information that could reasonably be considered confidential.~~

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

4. Audits referred to **in** paragraph 1 shall be performed by auditing organisations that:

(a) are independent from, and do not have any conflicts of interest with, the cloud computing service provider concerned, and any legal person connected to that provider, in particular:

i. have not provided non-audit services related to the matters audited to the cloud computing service provider concerned or to any legal person connected to that provider in the 12-month period before the beginning of the audit, and have committed to not providing them with such services in the 12-month period after the completion of the audit;

ii. have not provided auditing services pursuant to this Article to the cloud computing service provider concerned or any legal person connected to that provider ~~in the 10-year~~**during a** period ~~before the beginning of the audit~~ **longer than 5 consecutive years**;

iii. are not performing the audit in return for fees that are contingent on the result of the audit;

(b) have proven expertise, technical competence and capabilities in auditing cloud computing services;

(c) have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards.

5. Auditing organisations ~~that perform the audits~~ shall prepare an audit report for each audit. That report shall be substantiated, in writing, and shall include at least the following:

(a) the name, address and point of contact of the provider subject to the audit, and the period covered;

(b) the name and address of the auditing organisation or organisations performing the audit;

(c) a declaration of interests;

(d) a description of the specific aspects audited, and the methodology applied;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(e) a description and a summary of the main findings drawn from the audit;

(f) a list of the third parties consulted as part of the audit;

(g) a 'positive' or 'negative' audit opinion and any information on whether the audited service of the audited provider complies with the applicable audit criteria for Union assurance level 2, 3 or 4 pursuant to Annex II;

(h) where the audit opinion is 'negative', operational recommendations on specific measures to achieve compliance and the recommended timeframe to achieve compliance;

(i) where the audit opinion is 'positive', the Union assurance level that needs to be recognised under Article 17, issued to the audited service of the audited provider pursuant to the applicable criteria set out in Annex II.

6. Where the auditing organisation was unable to audit certain aspects or to express an audit opinion based on its investigations, the audit report shall include an explanation of the circumstances and the reasons why those aspects could not be audited.

7. The auditing organisation ~~may~~ **shall** revoke its audit report and audit opinion where the audited provider, intentionally or negligently, supplied incorrect or misleading audit evidence **that may affect the audit report and positive audit opinion**. **The auditing organisation shall inform the competent authority of establishment without undue delay.**

8. **Every two years** the audited provider shall ~~annually~~ submit for review the audit report and the associated 'positive' audit opinion to the same or a different auditing organisation which shall assess the continued compliance of the audited service with the applicable criteria set out in Annex II. On the basis of the ~~annual~~ review, the auditing organisation may confirm, update, or revoke the initial audit report and audit opinion.

9. The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by laying down rules on the performance of audits**,** on the procedural steps, rules for auditing organisations and their technical competences, auditing methodologies and templates for the audit reports.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

Article 21

Content and quality of audit evidence

1. 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 Commission is empowered to adopt delegated acts in accordance with Article 45 to amend Annex III by laying down the necessary evidence needed to assess the audit criteria under Annex II.~~

2. The audit evidence shall be:

   (a) relevant and sufficient to enable the auditing organisation to prepare an audit report and provide an audit opinion; and

   (b) reliable, according to the auditing organisation's professional judgment and scepticism.

Article 22

Central repository of cloud computing services

1. The Commission shall establish and maintain a dedicated repository of cloud computing services that have been recognised in accordance with Article 17 ('central repository').

2. The ~~national~~ competent authority of establishment that recognised a cloud computing service under Article 17 shall register the cloud computing service in the central repository.

3. ~~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 **without delay** in the central repository and shall remain ~~available there~~ **visible** for five years.

4. The central repository shall be publicly available **on a dedicated and easily accessible website** and regularly updated by the Commission and the ~~national~~ competent authorities ~~of establishment on a dedicated and easily accessible website~~.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Article 23

Transparency obligations

1. On becoming aware of any information or any material change in circumstances that may affect the audit report and the 'positive' opinion ~~under Article 20~~ or the recognition ~~under Article 17, the recognised~~ **decision, the** cloud computing service provider shall **without delay, and at the latest within 7 days,**~~, as soon as possible~~, notify the auditing organisation and the ~~national~~ competent authority of establishment.

2. On the basis of the notification under paragraph 1, the auditing organisation shall assess whether the audit report or the audit opinion need to be amended or revoked. Where the auditing organisation amends or revokes the audit report or the audit opinion, it shall~~, as soon as possible,~~ notify **without delay** the ~~national~~ competent authority of establishment.

3. On the basis of the notification referred to in paragraph 1 or 2, the ~~national~~ competent authority of establishment shall assess whether its recognition **decision** needs to be ~~amended~~ **suspended** or revoked **under Article 17a**. ~~Where the national competent authority of establishment amends or revokes it recognition of the cloud computing service, it shall, as soon as possible, notify the national competent authorities of the other Member States and the Commission.~~

Article 24

Penalties and compensation

1. Member States shall lay down the rules on penalties applicable to infringements of this Chapter by cloud computing service providers within their competence and shall take all measures necessary to ensure that they are implemented. ~~The~~ **Those** penalties ~~provided for~~ shall be effective, proportionate and dissuasive. Member States shall~~, as soon as possible,~~ **without delay** notify the Commission of those rules and ~~of those~~ measures and shall notify the Commission of any subsequent amendment affecting them.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

2. Member States shall take into account the following non-exhaustive criteria for the imposition of penalties for infringements of this ~~Regulation~~ **Chapter**:

(a) the nature, gravity, scale and duration of the infringement;

(b) any action taken by the infringing party to mitigate or remedy the damage caused by the infringement;

(c) any previous infringements by the infringing party;

(d) the financial benefits gained or losses avoided by the infringing party due to the infringement, insofar as such benefits or losses can be reliably established;

(e) any other aggravating or mitigating factor applicable to the circumstances of the case;

(f) infringing party's annual turnover in the preceding financial year in the Union.

2a. Member States shall ensure that infringements of this Chapter by cloud computing service providers are subject to administrative fines of a maximum of EUR 1 000 000 or 1% of the total worldwide annual turnover of the cloud computing service provider in the financial year preceding the year in which the infringement occurred, whichever is higher.

3. Recipients of the cloud computing services shall have the right to seek, in accordance with Union and national law, compensation from cloud computing service providers for any damage or loss suffered due to an infringement by those **cloud computing service** providers of their obligations under this Chapter.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

SECTION 4

NATIONAL COMPETENT AUTHORITIES

Article 25

~~National~~ Competent authorities

1. By [P.O. insert date of entry into force plus 1 year], Member States shall designate one or more national competent authorities responsible for enforcing this Chapter. To that effect, Member States may designate an existing authority or existing authorities ('competent authorities').

2. Member States shall notify the Commission of the names of the competent authorities and of their tasks and powers. The Commission shall maintain a public register of those authorities.

3. Member States shall ensure that their competent authorities perform their tasks under this Regulation in an impartial, transparent and timely manner. Member States shall ensure that their competent authorities have all necessary resources to carry out their tasks, including sufficient technical, financial and human resources to adequately supervise all cloud computing service providers within their competence.

4. The Member State in which the cloud computing service provider has its main establishment, that is, where the cloud computing service provider has its head office or registered office from which the principal financial functions and operational control are exercised, shall have exclusive competence for enforcing this Chapter.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Article 26

Powers of the ~~national~~ competent authorities

1. Where needed to carry out their tasks under ~~Article 17~~**this Chapter**, competent authorities of establishment shall have the following investigative powers:

   (a) the power to require any cloud computing service provider, as well as any other persons acting for purposes related to their trade, business, craft or profession, who may reasonably be expected to be aware of information relating to a suspected infringement of this Regulation, including auditing organisations, to provide that information ~~as soon as possible~~ **without delay**;

   (b) the power to carry out, or to request a judicial authority in their Member State to order, inspections of any premises that those providers or those persons ~~acting for purposes related to their trade, business, craft or profession,~~ use for purposes related to their trade, business, craft or profession, or to request other public authorities to do so, in order to examine, seize, take or obtain copies of information relating to a suspected infringement in any form, irrespective of the storage medium;

   (c) the power to ask any member of staff or representative of those providers or those persons ~~acting for purposes related to their trade, business, craft or profession~~, to give explanations in respect of any information relating to a suspected infringement and, with their consent, to record their answers by any technical means.

2. Where needed to carry out their tasks under ~~Article 17~~**this Chapter**, ~~national~~ competent authorities of establishment shall have the following enforcement powers:

   (a) the power to order the cessation of infringements and, where appropriate, to impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end, or to request a judicial authority in their Member State to do so;

   (b) the power to impose fines, or to request a judicial authority in their Member State to do so, for failure to comply with this ~~Regulation~~ **Chapter**, including with any of the investigative orders issued pursuant to paragraph 1;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(c) the power to impose a periodic penalty payment, or to request a judicial authority in their Member State to do so, in accordance with Article 24 to ensure that an infringement is terminated in compliance with an order issued pursuant to point (a), or for failure to comply with any of the investigative orders issued pursuant to paragraph 1.

3. Measures taken by ~~national~~ competent authorities of establishment in exercising their powers listed in paragraphs 1 and 2 shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement or suspected infringement to which those measures relate, and, where relevant, the economic, technical and operational capacity of the service provider concerned.

4. Member States shall set out specific rules and procedures for the exercise of the powers pursuant to paragraphs 1 and 2 and shall ensure that any exercise of those powers is subject to adequate safeguards under applicable national law in compliance with the general principles of Union law. Those measures shall be taken only in accordance with the right to respect for private life and the rights of defence, including the rights to be heard and to have access to the file, and shall be subject to the right of all affected parties to an effective judicial remedy.

SECTION 5

MUTUAL ASSISTANCE AND COOPERATION

Article 27

Mutual assistance

1. Competent authorities and the Commission shall cooperate closely and provide each other with mutual assistance to apply this Chapter in a consistent and efficient manner. Mutual assistance shall include the exchange of information.

2. A competent authority **of establishment** may request other competent authorities to provide specific information in their possession relating to a specific cloud computing service provider **or** to exercise its investigative powers under Article 26 regarding specific information located in their Member State. Where appropriate, the competent authority receiving the request may involve other competent authorities or other public authorities of the Member State in question.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

3. The competent authority receiving the request pursuant to paragraph 2 shall comply with such request and inform the competent authority of establishment about the action taken, as soon as possible and no later than two months after receipt of the request, unless duly justified.

Article 28

Cross-border cooperation

1. Where a competent authority ~~of destination~~ has reason to suspect that a cloud computing service provider no longer fulfils the ~~requirement~~ **requirements** under Annex II ~~to this Regulation~~, it may request the competent authority of establishment to assess the matter and to take the necessary investigatory and enforcement measures to ensure compliance.

2. The Commission may also request the competent authority ~~referred to in Article 25~~**of establishment** to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance.

3. Requests pursuant to paragraph 1 or 2 shall be duly reasoned and shall ~~be duly taken into account by the competent authority of establishment. Where~~ **indicate at least: (a) a description of the relevant facts, the requirements of Annex II concerned, and the reasons why** the competent authority ~~of establishment~~ **that sent the request or the Commission** considers that the ~~information provided is insufficient, it may either request additional~~ **cloud computing service provider no longer fulfils those requirements; (b) any other** information~~. The period set out in paragraph 4 shall be suspended until that additional~~ **that the competent authority that sent the request or the Commission considers relevant, including where appropriate** information ~~is provided~~ **gathered on its own initiative or suggestion for specific investigatory or enforcement measures to be taken, including interim measures.**

3a. The competent authority of establishment shall take utmost account of the requests pursuant to paragraph 1 and 2. Where the competent authority of establishment considers that the information provided is insufficient, it may request additional information. The period set out in paragraph 4 shall be suspended until that additional information is provided

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

4. The competent authority of establishment shall, ~~as soon as possible~~ **without delay** and in any event not later than two months after receipt of the request pursuant to paragraph 1 or 2, communicate to the competent authority that sent the request, and the Commission, its assessment of the suspected infringement and an explanation of any investigatory or enforcement measures taken or envisaged in relation to the matter to ensure compliance with this ~~Regulation~~ **Chapter**.

Article 28a

Professional secrecy

1. The Commission, the competent authorities of Member States, and any other natural or legal person involved, including auditing organisations referred to under Article 20, shall not disclose information acquired or exchanged by them pursuant to this Regulation and of the kind covered by the obligation of professional secrecy to any other person or authority except by virtue of the obligations laid down in this Regulation or the laws, regulations or administrative procedures of a Member State.

2. The exchange and use of information pursuant to this Chapter between the Commission, competent authorities, auditing organisations and other natural or legal persons referred to in paragraph 1 shall not be deemed to infringe the requirements of professional secrecy.

Article 28b

Information sharing system

1. The competent authorities and the Commission shall use reliable and secure information sharing systems for all communications pursuant to this Chapter.

2. The Commission shall adopt implementing acts laying down the practical arrangements for the sharing of information referred to in paragraph 1, including the use of dedicated information sharing systems and conditions of the information-sharing arrangements. In laying down the information-sharing arrangements, the Commission may establish a dedicated information sharing system or select or make use of existing information sharing systems. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

Chapter II

Demand-side measures

SECTION 1

PUBLIC PROCUREMENT

Article 29

Risk assessments

1. By [date of entry into force plus 1 year], and thereafter every two years, or whenever necessary, Member States and Union entities shall carry out risk assessments that shall:

   (a) identify the public sector activities that use or will make use of cloud computing services, **and** that contribute to the preservation of public order in sectors falling under Annex I or II of Directive (EU) 2022/2555 ~~and~~ **or** in the areas of ~~national security,~~ internal security, external border management~~, defence~~, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal ~~offence~~ **offences**;

   (b) determine which Union assurance level 2, 3, or 4 set out in Annex II of this Regulation is appropriate for the identified public sector activities.

   Where Union entities and Member States share responsibilities in relation to the public sector activities, they shall, where appropriate, consider carrying out the relevant risk assessment or assessments jointly.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

2. In carrying out their risk assessments **referred to in paragraph 1**, Member States and Union entities shall consider at least the following ~~aspects~~ **elements**:

   (a) the sensitivity, criticality, and ~~magnitude~~ **volume** of the **personal data and** non-personal data **stored or** processed, including the potential impact on public order**,** and the nature, scope, context and purpose of processing of **the** personal data~~, as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects~~;

   (b) the risk and consequent impact on public order of unlawful access under Union law to such data by a third country or a legal entity established in a third country;

   (c) the risk and consequent impact on public order of possible service disruption;

3. **By [date of entry into force plus 6 months],** the Commission shall~~,~~ by means of implementing acts ~~in accordance with Article 46(2),~~ specify the methodology to be applied, the templates to be used and the elements to be taken into account by the Member States and Union entities— for the purpose of carrying out the risk assessments referred to in paragraph 1. The methodology shall ~~specify how~~ **guide** Member States ~~use the highest level of~~ **and Union entities when determining the appropriate Union** assurance **level** for the most critical public sectors activities**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2)** ~~including, but not limited to, defence~~.

4. Within three months of carrying out the risk assessments referred to in paragraph 1, Member States shall provide the Commission with the results of those risk assessments, indicating where they depart from the implementing acts referred to in paragraph 3. **The information provided by the Member States to the Commission shall be limited to what is necessary for the purposes of this Regulation and may be provided in aggregated or summarised form where disclosure of information could create security risks or conflict with national confidentiality requirements.**

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

5. ~~If~~ **Where** the Commission ~~concludes~~ **finds**, after reviewing the results of the risk ~~assessment or~~ assessments of ~~a~~ **one or more** Member ~~State~~ **States**, that the Union assurance level identified for the public sector activity ~~in a risk assessment~~ is not appropriate ~~or does not adequately address the public order concerns~~**, it may issue recommendations to the concerned Member States or for the Union as a whole. Where recommendations are issued by the Commission**, **the concerned Member States shall, within three months of receipt of the recommendations, notify** the Commission ~~may adopt implementing acts in accordance with Article 46(2) specifying the Union assurance levels needed for the public sector activity~~ **on how they intend to take due account of the recommendations**.

6. Where ~~the risk assessment requires~~ the migration to another cloud computing service **is required**, the Member State or Union entity shall migrate within a reasonable transition period that shall not exceed ~~12~~**18** months, taking into account technical feasibility, continuity of service and data portability requirements applicable to such migration. **By way of exception, that period may be extended only to the extent strictly necessary where compliance within 18 months is not reasonably feasible.**

7. Member States shall cooperate with each other and with the Commission through established consistency mechanisms and promote cooperation and effective exchange of information and best practices.

8. For the purpose of paragraph 3, the Commission shall be empowered to request cloud computing service providers to provide all the necessary information.

9. In their risk assessments, Member States and Union entities shall consider whether a multi-vendor or multi-cloud strategy is appropriate as part of their procurement of cloud computing services.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Article 30

Public procurement

1. This Article applies to ~~contracting authorities that procure~~ **public procurement procedures of** cloud computing services ~~for their exclusive use~~ **falling within the scope of Directive 2014/24/EU or Directive 2014/25/EU**. Without prejudice to Article 136 of Regulation (EU, Euratom) 2024/2509, this Article also applies to ~~Union entities that procure~~ **public procurement procedures of** cloud computing services ~~for their exclusive use~~ **by Union entities**.

2. Union entities**, contracting authorities, and contracting entities** ~~and public sectors bodies~~ whose public sector activities have ~~not~~ been identified as contributing to the preservation of public order **but have not been identified** under the risk ~~assessment~~ **assessments** referred to in Article 29(1) **as requiring Union assurance levels 2, 3 or 4** shall ~~use~~ **procure** cloud computing services that have been recognised ~~under Article 17~~ as having a Union assurance level 1.

3. **Union entities,** contracting authorities, ~~including the~~ **and contracting** entities ~~acting on their behalf,~~ whose activities have been identified as contributing to the preservation of public order under Article 29(1) in sectors falling under Annex I or II of Directive (EU) 2022/2555 ~~and~~ **or** in the areas of ~~national security,~~ internal security, external border management~~,~~ ~~defence~~, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal ~~offence~~ **offences**, shall ~~only~~ procure cloud computing services that have been recognised as having a Union assurance level 2, 3 or 4.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

4. By **way of** derogation from paragraphs 2 or 3, on an exceptional basis and where duly justified, **Union entities,** contracting authorities **and contracting entities** may decide not to procure cloud computing services recognised as having a Union assurance level 1, 2, 3, or 4 where one or more of the following circumstances applies:

(a) the subject matter of the ~~tender~~ **contract** cannot be supplied by ~~recognised~~ **a cloud computing service provider with** cloud computing services ~~available in the central repository referred to in Article 22~~**recognised at the necessary Union assurance level**, and no ~~adequate or~~ reasonable alternative or ~~comparable~~ **substitute** cloud computing service exists, and ~~such~~ **the** absence **of competition** is not the result of an artificial narrowing down of the parameters of the public procurement procedure;

(b) the **Union entity,** contracting authority **or contracting entity** has launched a similar procurement ~~process~~ **procedure** within the previous ~~year but did not receive any~~**24 months but no** suitable tenders or suitable ~~participants~~ **requests to participate were submitted**;

(c) applying the requirements of this ~~Regulation~~ **Chapter** would require **the Union entity,** the contracting authority**, or the contracting entity** to procure **cloud computing** services at disproportionate cost.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

SECTION 2

PRIVATE SECTOR ENTITIES

Article 31

~~Impact~~ Risk assessments for private sector entities

1. Entities ~~referred to~~ **listed** in Annex I of Directive (EU) 2022/2555 who are not public sector bodies **('private sector entities operating in sectors of high criticality')** may carry out similar **risk** assessments as those set out in Article 29.

2. The Commission may issue guidance on the methodology for carrying out ~~the impact~~ **those risk** assessments ~~under this Article~~ and possible mitigation measures to be adopted by private sector entities operating in sectors of high criticality.

3. ~~Where, because of specific circumstances, and where duly justified and in consultation with the Member States, the Commission concludes that entities who are not public sector bodies operating in sectors of high criticality require an impact assessment, the Commission may adopt delegated acts to supplement this Regulation in accordance with Article 45 specifying the need for such impact assessment and the risk mitigation measures that those entities who are not public sector bodies shall take.~~

SECTION 3

OTHER PROCUREMENT-RELATED MEASURES

Article 32

Union added value

1. In public procurement procedures for innovative cloud computing services ~~and~~ **or** AI systems, **Union entities and** contracting authorities shall include, as part of the quality evaluation of the tender, non-price award criteria that allow them to evaluate the tenderer's contribution to the development of a European cloud and AI ecosystem.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

2. ~~When applying non-price award criteria under paragraph 1, contracting authorities shall ensure that non-price award criteria are:~~

   (a) ~~linked to the subject matter of the contract;~~

   (b) ~~not conferring unrestricted freedom of choice on the contracting authority;~~

   (c) ~~expressly set out in the procurement documents or in the contract notice;~~

   (d) ~~ancillary and not decisive in the award of the contract.~~

3. Without affecting **Union entities and** contracting authorities~~'~~**'** discretion to apply additional criteria, the non-price award criteria referred to in paragraph 1 shall enable contracting authorities to evaluate the extent to which:

   (a) the ~~tenderer~~ **tender** contributes to strengthening the digital technology supply chain in the Union, including the use of software or hardware designed or manufactured in the Union;

   (b) the ~~tenderer has integrated~~ **tender integrates** technologies developed in the Union, including research and development results stemming from Union funded research and development programmes and makes use of tools, such as standards, ~~specification~~ **specifications**, software, models or other technology developed in the Union;

   (c) the innovation required to deliver the service contributes to strengthening the security of supply and the development of a European cloud and AI ecosystem;

   (d) the service is delivered, to the greatest extent feasible with regard to market availability and technical requirements, through critical computing, storage and networking hardware components designed and/or manufactured in the Union, or, where this is not feasible, through hardware components from a third country that contributes to strengthening the security of supply and the development of a European cloud and AI ecosystem.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Article 33

Monitoring of procurement of innovation in cloud and AI

1. **On the basis of available information,** Member States shall monitor and report on their use of procurement of innovation in cloud computing services and AI systems.

2. ~~Member States shall take appropriate measures to ensure that the monitoring and reporting referred to in paragraph 1 are actively used to identify barriers to SMEs participation in procurement procedures, to improve access of SMEs to procurement markets, support the design of simplified, proportionate and SME-friendly procurement strategies, including division into lots, where appropriate, promote the participation of SMEs in the innovation procedure foreseen under Directive 2014/24/EU and pre-commercial procurement of cloud computing services and AI systems.~~

3. Based on the monitoring referred to in paragraph 1, Member States shall**, every three years,** inform the Commission~~, on a yearly basis,~~ of the following information:

   (a) the size of the economic operators participating in such procurement;

   (b) ~~SMEs~~ **SME, startups and scaleups** participation trends, including the number of contracts awarded to SMEs **startups and scaleups**, their share of the total contract value, as a percentage, and, where available, the share of cross-border ~~SMEs~~ **SME, startups and scaleups** participation;

   (c) measures taken to improve ~~SMEs~~ access to public procurement procedures **for SMEs, startups and scaleups**.

4. Member States shall pursue as objective that ~~at least 25%~~**an adequate percentage** of their procurement for cloud computing services and AI systems be awarded to innovative SMEs**, startups and scaleups**.– Member States shall include, in their national strategies referred to in Article 7, plans on how they intend to achieve this objective.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

5. Union entities and contracting authorities shall promote:

(a) ~~preliminary market consultations;~~

(b) matchmaking between public buyers and innovative solutions provided by European SMEs**, startups and scaleups**~~ and start-ups~~;

(c) development of public contract clauses that are favourable for innovative SMEs**, startups and scaleups**.

Chapter III

European public sector cloud federation

Article 34

Establishment of the European public sector cloud federation

1. The European public sector cloud federation (the 'EuroCloud Federation') is hereby established. The EuroCloud Federation shall be open for the participation of Union entities and public sector bodies on a voluntary basis. Union entities and public sector bodies may request the Commission to join the EuroCloud Federation.

2. The EuroCloud Federation shall facilitate the sharing of public sector data centre services and cloud computing services between Union entities and public sector bodies under the conditions set out in Articles 35 and 36.

3. The Commission shall establish a platform for the EuroCloud Federation**, which may provide interoperability with existing platforms and systems, and** providing at least:

(a) a catalogue providing information on available public sector data centre services and cloud computing services;

(b) a service platform for the exchange and orchestration of computing, storage and network resources and services;

(ba) mechanisms to ensure secure access and service management, including shared identity and access management, shared authentication mechanisms and service management reporting tools;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(bb) capabilities supporting the operations of provided services, including monitoring of service provision, resource allocation, service activation and monitoring.

4. The Commission is empowered to adopt implementing acts to specify the procedure to participate in the EuroCloud Federation and ~~template~~ **templates** concerning the content and other details of the request for participation. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Article 35

Sharing of public sector data centre services and cloud computing services

1. A member of the EuroCloud Federation (the 'sharing entity') may share data centre services and cloud computing services **(the 'services')** with another member of the EuroCloud Federation (the 'using entity') where the sharing entity directly, or indirectly through an intermediate legal entity, ~~owns the hardware~~ **operates the physical assets** through which the ~~service is~~ **services are** made available and provides the service that ~~is~~ **are** made available to the using entity. Where the sharing entity ~~indirectly owns the hardware~~ **operates the physical assets** and provides the services **indirectly** through an intermediate legal entity, the sharing entity shall exercise control over that intermediate legal entity. **The sharing entity shall be deemed to exercise control over that intermediate legal entity within the meaning of this paragraph where the following conditions are fulfilled:**

(a) the sharing entity exercises a decisive influence over the strategic objectives and significant decisions of that intermediate legal entity;

(b) there is no direct private capital participation in that intermediate legal entity; and

(c) more than 80% of the activities of that intermediate legal entity are carried out performing tasks entrusted to it by the sharing entity.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

2. The sharing entity shall put in place appropriate technical, operational and organisational measures to ensure an effective, secure and resilient provision of services. **The technical, operational and organisational measures referred to in this paragraph shall include at least the following:**

   (a) internal governance and control frameworks, setting clear roles and responsibilities for ICT-related functions and access control policy management;

   (b) policies on risk analysis and information system security;

   (c) policies ensuring high standards on integrity and confidentiality of data;

   (d) policies supporting interoperability and connectivity.

3. Prior to sharing ~~data centre services and cloud computing~~ services within the EuroCloud Federation, the sharing entity shall demonstrate to the Commission that it fulfils the conditions set out in paragraphs 1 and 2.

4. The Commission shall assess the information provided by the sharing entity and ~~allow~~ **authorise** the sharing entity to share ~~data centre services and cloud computing~~ services within the EuroCloud Federation where the conditions laid down in paragraphs 1 and 2 are fulfilled. **The sharing entity shall inform, without delay, the Commission of any material change that may affect the authorisation granted.**

The Commission may revoke or suspend the authorisation to share services within the EuroCloud Federation where the sharing entity no longer fulfils the conditions laid down in paragraphs 1 and 2.

5. The sharing entity may charge a fee to the using entity. The amount of the fee shall be limited to the costs that the sharing entity incurs in relation to the sharing of the service and shall not constitute a pecuniary interest within the meaning of Article 2 of Directive 2014/24/EU and Regulation (EU, Euratom) 2024/2509.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

6. The Commission is empowered to adopt implementing acts to specify the technical, operational and organisational measures referred to in paragraph 2. **The Commission shall take into account the extent to which those measures are already covered in requirements laid down in Union law.** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Article 36

Fees for the administration of the EuroCloud Federation

1. The costs arising from the activities carried out by the Commission pursuant to this Chapter shall be jointly financed by the members of the EuroCloud Federation through fees levied by the Commission. **The fees shall be set in advance, shall be proportionate to the estimated costs of the activities for which fees are chargeable as determined in a cost-effective way, and shall be sufficient to cover those costs.**

2. If the costs are initially borne by the general budget of the Union, they shall be reimbursed by the EuroCloud members over a period not exceeding three years from the date on which the costs were borne by the Union.

3. Revenues generated by the fees shall constitute internal assigned revenues within the meaning of Article 21(3), point (a), of Regulation (EU, Euratom) 2024/2509. Those revenues shall be assigned to cover the costs of the activities carried out by the Commission pursuant to this Chapter, including assessing ~~request~~ **requests** to join the EuroCloud Federation and the establishment of the platform referred to in Article 34(3). Any revenue remaining after covering those costs shall be entered into the general budget of the Union.

4. The Commission shall adopt implementing acts laying down detailed rules for determining the estimated costs, the individual amount of the fees, and the manner and conditions under which the fees are to be paid. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Chapter IV

Procurement of data centre services, cloud computing services, software ~~and~~, AI systems and AI models by the Commission

Article 37

Procurement activities of the Commission

1. The Commission may carry out procurement activities to procure data centre services, cloud computing services, software ~~and~~, AI systems **and AI models (supplies and services)** for itself and ~~forUnion entitiesand~~ **for Union entities and** for contracting authorities of Member States~~,~~, in accordance with Regulation (EU, Euratom) 2024/2509, subject to the exceptions set out in this Chapter. By way of derogation from Article 168 of Regulation (EU, Euratom) 2024/2509, partner organisations referred to in Article 168(3) of that Regulation selected by the Commission may also participate in the procurement activities set out in this Chapter. Contracting authorities of Member States, Union entities, and partner organisations selected by the Commission, shall be considered as 'participating entities' under this Chapter. **Participation in procurement activities carried out by the Commission under this Chapter shall remain voluntary for participating entities.**

2. Contracting authorities may participate in the procurement procedures on their own behalf, or as central purchasing bodies within the meaning of Article 2(1), point (16) of Directive 2014/24/EU when they qualify as such. Specific rules and obligations governing their participation may be imposed where they participate as central purchasing bodies in the agreement referred to in Article 38.

3. In addition to the procurement activities provided for in Article 168 of Regulation (EU, Euratom) 2024/2509, the Commission may act as a central purchasing body for contracting authorities of Member States and partner organisations selected by the Commission, by:

   (a) procuring ~~data centre~~ services~~, cloud computing services, software and AI systems~~ **and supplies** on behalf of, or in the name of, one or more contracting authorities of Member States and partner organisations selected by the Commission, by concluding framework contracts or operating dynamic purchasing systems for services **and supplies** intended for the participating entities;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(b) acting as a wholesaler by acquiring ~~such~~ services and supplies and reselling them or, in exceptional circumstances, donating them to one or more contracting authorities of Member States.

4. In carrying out procurement activities, the Commission may provide ancillary support to participating entities, including:

(a) technical infrastructure enabling participating entities to use awarded contracts or award contracts, including specific contracts under concluded framework ~~agreements, for data centre~~ **contracts, for** services~~, cloud computing services, software and AI systems~~ **and supplies**;

(b) advice and support on preparing and implementing procurement procedures;

(c) preparation and conduct of procurement procedures on behalf of, or in the name of, the entities concerned;

(d) invoicing and other administrative services relating to the contracts awarded.

5. Such ancillary support may be provided directly by the Commission, through a subcontractor, or by delegation to Union bodies or agencies. Accession of participating entities to the agreement referred to in Article 38 may be subject to the acceptance of one or more ancillary support services**, where those services are necessary for the participation in the procurement activities concerned and this requirement is proportionate**.

6. The Commission may establish and manage a common procurement platform including services that may be used to facilitate the procurement activities under this Chapter. **The common procurement platform may provide interoperability with existing platforms and systems.**

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Article 38

Arrangements for the procurement activities by the Commission

1. Before any procurement activity to be carried out under Article 37, the Commission and at least two Member States shall enter into an agreement laying down the practical arrangements for the procurement activities carried out by the Commission under this Chapter. The agreement shall cover procurement procedures to be carried out during its period of validity and shall be deemed to satisfy the requirements of the joint procurement agreement and **of the** mandate **to procure on behalf of or in the name of participating entities, respectively** referred to in Article 168(2) and (3)**, point (e)** of Regulation (EU, Euratom) 2024/2509.

2. ~~The agreement shall constitute a mandate for the Commission to procure on behalf of, or in the name of, the participating entities within the meaning of Article 168(3), point (e), of Regulation (EU, Euratom) 2024/2509.~~

3. The agreement shall include the practical arrangements for the participation of entities, the **conditions and time frames for possible opt-in and opt-out, the** decision-making process for the choice of procedure and the applicable conditions**, including those related to the division of responsibilities between the Commission and participating entities**, the evaluation of requests for participation and tenders, the award of contracts, and the applicable law and competent jurisdiction. ~~The Commission shall remain responsible for the operation and management of procurement activities, including for deciding on the launch of a procurement procedure, the type of procedure and of contract, and the award of contracts.~~

4. The agreement shall establish a Steering Committee composed of the Commission and one representative from each participating Member ~~States~~ **State** at national level. Member States may accede to the agreement at a later stage and shall then be represented in the Steering Committee. The Steering Committee may appoint additional representatives of other Union entities, of contracting authorities of Member States and of partner organisations selected by the Commission.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

5. The Steering Committee shall be responsible for the strategic oversight of the procurement activities, including for proposing the strategic direction of ~~the~~ procurement ~~agenda for a fixed period, and for approving the strategic direction of each procurement procedure~~ **procedures** before ~~it is~~ **they are** launched by the Commission, to ensure ~~its~~ **their** compliance with the framework established by this Regulation. **The Steering Committee shall be informed of the scope of procurement procedures. The Commission shall remain responsible for the operation and management of procurement activities, including for deciding on the launch of a procurement procedure, the type of procedure and of contract, and the award of contracts. In particular, the Commission may decide to launch a procurement procedure open to participating entities without a prior specific request from them.**

6. Once the agreement has entered into force, contracting authorities of ~~participating~~ Member States, Union entities and partner organisations selected by the Commission may accede to and benefit from it and shall be considered as participating entities in the procedures in which they elect to participate. The Steering Committee may determine that the agreement shall take the form of a contract of adhesion.

7. The participation of a contracting authority of a Member State shall not be conditional on that Member State's participation**, provided this is not contrary to the applicable national law**.

8. The Steering Committee shall set transparent ~~and~~**,** non-discriminatory **and objective** conditions for contracting authorities of Member States to accede to the agreement~~, in particular as regards size, minimum amounts and other objective criteria~~. The Steering Committee shall also set out the rules and procedures governing the termination of participation in the agreement of a contracting authority of a Member State that has failed to comply with its obligations under the agreement.

9. By way of derogation from Article 168(2) of Regulation (EU, Euratom) ~~2014/2509~~**2024/2509**, the Steering Committee may approve the participation of contracting authorities from EFTA States and Union candidate countries without the need for a bilateral or multilateral treaty ~~provided~~ **to provide** for such **a** possibility.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

10. The Steering Committee may make accession to the agreement conditional on participating entities accepting one or more ancillary support services, **where those services are necessary for the participation in the procurement activities concerned and this requirement is proportionate,** as set out in Article 37.

11. The Steering Committee shall adopt its rules of procedure, following a proposal from the Commission.

Article 39

Applicable public procurement framework

1. A participating entity shall be deemed to have fulfilled its obligations under applicable Union public procurement law where it acquires supplies or services by means of contracts awarded by the Commission under this Chapter, including through framework contracts concluded by or dynamic purchasing systems operated by the Commission acting as a central purchasing body, or any ancillary support services referred to in Article 37.

2. The procedural provisions applicable to Union institutions shall apply to the procedures for the award of specific contracts under framework contracts or dynamic purchasing systems.

3. A contracting authority that has acquired ~~data centre~~ services~~, cloud computing services, software and AI systems~~ **and supplies** from the Commission as a central purchasing body **may offer those services and supplies to other contracting authorities without applying the public procurement procedures provided for under applicable Union law. In that case, the contracting authority** shall ensure, in its agreements with the contracting authorities it serves, compliance with any contractual requirements by which it is itself bound.

4. ~~The Commission may decide to launch a procurement procedure open to participating entities without a prior specific request from them.~~

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

5. By way of derogation from Article 168 of Regulation (EU, Euratom) 2024/2509, participating entities may request from the Commission, throughout the period of validity of a dynamic purchasing system, the possibility to participate in the system. Such request shall be approved by the Commission provided that the cumulative requests do not exceed 50% of the initial estimated quantities of the envisaged purchases. The participation shall be approved within 10 working days of receipt of the request and shall allow the participating entities to be included in any future invitation to tender.

6. The possibility referred to in paragraph 5 shall be available only to participating entities that accede to the agreement referred to in Article 38 after the dynamic purchasing system has been launched.

Article 40

Fees for procurement activities

1. The costs arising from the procurement activities carried out pursuant to this Chapter shall be jointly financed by the participating entities through fees levied by the Commission.

2. The costs incurred in establishing the common procurement activities referred to in Article 37, including the development of the common procurement platform, may be initially borne by the general budget of the Union. In such case, they shall be reimbursed by the participating entities over a period not exceeding three years from the date on which they were borne by the Union. The Commission may adopt implementing acts laying down the practical and operational arrangements for reimbursement by the participating entities. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

3. Revenues generated by the fees shall constitute internal assigned revenues within the meaning of Article 21(3), point (a), of Regulation (EU, Euratom) 2024/2509. Those revenues shall be assigned to cover the costs of the procurement activities carried out pursuant to Article 37. Any revenue remaining after covering those costs shall be entered into the general budget of the Union.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

4. The fees shall be set in advance, shall be proportionate to the estimated costs of the activities for which fees are chargeable as determined in a cost-effective way, reflecting practices of comparable procurement frameworks, and shall be sufficient to cover those costs.

5. ~~5.~~ The Commission shall adopt implementing acts laying down detailed rules for determining the fees, specifying the following:

   (a) the estimated costs attributable to the procurement activities for which fees are chargeable;

   (b) the individual amounts of the chargeable fees;

   (c) the manner and conditions under which the fees are to be paid;

   (d) ~~the conditions under which the fees are to be paid.~~

   When adopting the implementing acts referred to in this paragraph, the Commission may take into account several parameters, including: a) service consumption; b) usage commitment; c) maximum service fee.

   Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

Chapter V
Open source

Article 41

Promoting open source solutions ~~andopen source first~~

The Union and Member States shall take the necessary measures to encourage Union entities and public sector bodies to use and facilitate the reuse of open standards and components released under an open source licence when building their cloud and AI ecosystem or stack, taking into account functionalities, including security, total cost, **interoperability** and other relevant, duly justified objective criteria.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

Article 42

Share and reuse of software

When making software to which they hold intellectual property rights available for reuse under an open source licence, a Union entity or public sector body shall do so using a catalogue or repository that is connected to, and made accessible through, the EU OSS Catalogue referred to in Article 43.

Article 43

EU Open Source Solutions Catalogue

1. The Commission shall provide and maintain an EU Open Source Solutions Catalogue ('EU OSS Catalogue') as a ~~centralised~~ **federated** catalogue to access software made available for reuse by Union entities and public sector bodies.

2. The EU OSS Catalogue shall be hosted on the Interoperable Europe portal referred to in Article 8 of Regulation (EU) 2024/903 and shall be accessible electronically free of charge.

3. The Commission shall, on the basis of objective and relevant criteria, decide on the request of any Union entity or public sector body owning or maintaining a catalogue or repository to have that catalogue or repository connected to and made accessible through the EU OSS Catalogue.

Article 44

Network of Open Source Programme Offices

1. The Commission shall establish a network of Open Source Programme Offices ('OSPO Network') to facilitate cooperation on the implementation of the obligations under this Chapter.

2. Open Source Programme Offices established by public sector bodies at local, regional or national level in a Member State, and those established by Union entities, may request from the Commission to join the OSPO Network.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

3. The OSPO Network shall have the following tasks:

(a) facilitating the exchange of information, experience and best practices between Member States and the Commission, in particular by discussing common technical, legal and organisational challenges, including those related to licensing, security, maintenance and procurement of open-source software;

(b) promoting the sharing and reuse of open-source software by public sector bodies;

(c) contributing, on a voluntary and non-binding basis, to the development of guidance, templates or recommendations on the sharing and reuse of open-source software;

(d) collaborating on and exchanging open-source projects of common interest to Union entities and public sector bodies.

4. The Commission shall support and coordinate the OSPO Network.

5. The Commission shall convene and chair a meeting of the members of the OSPO Network at least twice a year. The meetings of the OSPO Network may be organised online.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

ANNEX II

Criteria For Union Assurance Levels

This Annex sets out the criteria to be met by cloud computing service providers and their cloud computing services in order to be recognised as offering services at Union assurance levels 1, 2, 3 ~~and 4.~~ **or 4.** For the purpose ~~of the criteria under Union assurance levels 1, 2, 3, and 4, 'software' within the meaning of Regulation (EU) 2024/2847, Article 3, point (4) falls within the scope~~ of this Annex and Annex III ~~to this Regulation. 'Hardware' within the meaning of Regulation (EU) 2024/2847, Article 3, point (5) is outside of the scope.~~**, the following definitions apply:**

(a) 'software' means software as defined in Article 3, point (4), of Regulation (EU)2024/2847. For the purpose of this Annex and Annex III, firmware is considered software;

(b) 'hardware' means hardware as defined in Article 3, point 5, of Regulation (EU) 2024/2847;

(c) 'component' means component as defined in Article 3, point (6), of Regulation (EU) 2024/2847;

(d) 'manufacturer' means manufacturer as defined in Article 3, point (13), of Regulation (EU) 2024/2847;

(e) 'customer' means a Union entity, a contracting authority or a contrating entity who has entered into a contractual or other legally binding arrangement with the cloud computing service provider for the purpose of accessing or using the cloud computing service;

(f) 'customer data' means any data under the control of the cloud computing service customer, whether by legal, contractual, or other means, that are input into the cloud computing service by or on behalf of the customer, including authentication credentials or produced through the customer's use of the cloud computing service. Customer data can 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);

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(g) 'cloud computing service derived data' means data that 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;

(h) 'telemetry data' means [...]

(i) 'metadata' means [...]

(j) 'infrastructure' means physical infrastructure, including but not limited to, data centre infrastructure or colocation infrastructure, network, cooling, and IT systems that allow for the management of the data centre;

(k) 'assets' means hardware and software, including, but not limited to, libraries, the internal network needed for software components to communicate, cryptographic materials that enables the provision of the cloud computing service;

(l) 'personnel', including personnel managed by subcontractors, means individuals who support the delivery, administration, security, availability, or operation of the audited service;

(m) 'subcontractors' means subcontractors that directly or indirectly contribute to the provision and the delivery of the cloud computing service or that may require access to classified or sensitive information.

1. Union assurance level 1

1.1. For Union assurance level 1, cloud computing service providers must meet the following cumulative criteria:

(a) the cloud computing service provider is established in the Union;

(b) the infrastructure and assets of the cloud computing service provider, including those of its subcontractors which are involved in the provision of the service, are located in the Union unless the ~~public sector body~~ **Union entity, the contracting authority or the contracting entity** explicitly ~~requires~~ **allows** otherwise;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(c) the customer data, including metadata and telemetry data, that is processed, stored and transferred by the cloud computing service provider, and by the subcontractors, which are involved in the provision of the service, remain exclusively within the Union, unless the ~~public sector body~~ **Union entity, contracting authority, or contracting entity** explicitly ~~requires~~ **allows** otherwise and at any time, including before, during or after the configuration or use of the service**. Subject to fully auditable transparency, monitoring and security obligations, metadata and telemetry data can be processed, stored or transferred outside of the Union to the extent strictly necessary and proportionate to ensure the cybersecurity protection of the cloud computing service, if that purpose cannot be reasonably achieved by processing such data within the Union and provided that such processing, storage or transfer does not disrupt service continuity and/or degrade the service quality**;

(d) where the cloud computing service provider outsources the technical and operational support or assistance, including any subsequent sub-outsourcing arrangements, to third-party service providers outside of the Union, the necessary legal, technical and organisational measures are implemented to ensure traceability, security and governance of those operations and those operations do not~~, in any way,~~ compromise the operational autonomy of the cloud computing service provider;

(e) the cloud computing service provider demonstrates that the service complies with the state-of-the-art cybersecurity standards;

(f) the cloud computing service provider provides full transparency around the use of subcontractors. The cloud computing service provider subjects subcontractors to due diligence, contractual obligations and ongoing oversight to meet Union legal obligations;

(g) Where the cloud computing service provider is subject to the control of a third country or a legal entity established in a third-country, the cloud computing service provider ~~guarantees~~ **demonstrates** that there are no existing laws and practices in that third country, demonstrated by independent sources, that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(ga) The cloud computing service provider supports standards-based integration of external identity providers for authentication and access management for the cloud service;

(gb) The cloud computing service provider provides customers with the capability to record, retain, and review logs of management and data access activities related to cloud service customer data. These logs should enable customers to identify when access occurred, the identity associated with the request, and the relevant operational context available through the service's logging capabilities;

1.2. ~~For Union assurance level 1, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship with the cloud computing service provider and that contribute to the provision and the delivery of the cloud computing service.~~

2. Union assurance level 2

2.1. For Union assurance level 2, cloud computing service providers must meet the following cumulative criteria:

(a) the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

(b) the infrastructure, assets, and personnel of the audited provider, including those of its subcontractors which are involved in the provision of the service are located in the Union;

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(c) the customer data, including metadata and telemetry data, that is processed, stored and transferred by the audited provider and the subcontractors which are involved in the provision of the service, remain exclusively within the Union, unless the ~~public sector body~~ **Union entity, the contracting authority or the contracting entity** explicitly ~~requires~~ **allows** otherwise and at any time, including before, during or after the configuration or use of the service**. Subject to fully auditable transparency, monitoring and security obligations, metadata and telemetry data can be processed, stored or transferred outside of the Union to the extent strictly necessary and proportionate to ensure the cybersecurity protection of the cloud computing service, if that purpose cannot be reasonably achieved by processing such data within the Union and provided that such processing, storage or transfer does not disrupt service continuity and/or degrade the service quality**;

(d) if the ~~public sector body~~ **Union entity, the contracting authority or the contracting entity** determines that imposing additional personnel screening and Union citizenship requirements are necessary, the audited provider ~~should~~ **must** ensure that ~~personnel~~ **personnel** meeting those requirements are available;

(e) the audited service obtains a European cybersecurity certificate of at least assurance level 'substantial' 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;

(f) the data generated by using the audited service are not used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country , and are not transferred outside the Union in any case;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(g) if the audited provider and the subcontractors– which are involved in the provision of the audited service are subject to the control of a third country or a legal entity established in a third-country, they demonstrate that the necessary legal, technical and organisational measures have been implemented to ensure that the:

i. control of the third country or the legal entity established in a third-country over the audited provider 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. access by a third country or by a legal entity established in a third-country to customer data is prevented;

iii. possibility of disruption of the service continuity and/or the degradation of the service quality by a third country or a legal entity established in a third country is prevented;

iv. ~~control of the third country or the legal entity established in a third-country over the audited provider 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~~

(ga) The cloud computing service provider supports standards-based integration of external identity providers for authentication and access management for the cloud service;

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(gb) The cloud computing service provider provides customers with the capability to record, retain, and review logs of management and data access activities related to cloud service customer data. These logs should enable customers to identify when access occurred, the identity associated with the request, and the relevant operational context available through the service's logging capabilities;

(h) the technical and operational support or assistance related to the audited service, including subsequent sub-outsourcing arrangements, are initiated and performed exclusively within the Union;

(i) **where software is not released under an open source licence,** the audited provider demonstrates that the following software supply chain measures are in place:

i. a complete and up-to-date software bill of materials (SBOM), ~~as defined in Article 3, point (39), of Regulation (EU) 2024/2847,~~and a list of identified dependencies relevant to the provision of the service are documented and made available to the auditing organisation;

ii. where software components ~~as defined in Regulation (EU) 2024/2847 Article 3, point 6~~ 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 software manufacturers~~, as defined in Regulation (EU) 2024/2847 Article 3, point 13,~~ 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;

iii. where the cloud computing service provider is subject to the control of a third country or a legal entity established in a third-country, the cloud computing service provider ~~guarantees~~ **demonstrates** that there are no existing laws and practices in that third country, demonstrated by independent sources, that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(j) where software released under an open-source licence is used for the provision of the service, the audited provider demonstrates that it has 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;

(k) to the extent that the audited provider provides its services ~~globally~~ **outside the Union** and maintains a subsidiary in a third country, the audited provider has implemented the necessary measures to ensure and enforce the effective legal, technical and organisational separation between the Union parent company and any ~~such~~ third-country subsidiary.

2.2. ~~For Union assurance level 2, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship to the cloud computing service provider and that contribute to the provision and delivery of the cloud computing service.~~

3. Union assurance level 3

3.1. For Union assurance level 3, cloud computing service providers must meet the following cumulative criteria:

(a) the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

(b) the infrastructure, assets, and personnel of the audited provider, including those of the subcontractors which are involved in the provision of the service, are located in the Union;

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(c) the customer data, including metadata and telemetry data, that is processed, stored and transferred by the audited provider and the subcontractors– which are involved in the provision of the service, remain exclusively within the Union unless the ~~public sector body~~ **Union entity, the contracting authority of the contracting entity** explicitly ~~requires~~ **allows** otherwise and at any time, including before, during or after the configuration or use of the service**. Subject to fully auditable transparency, monitoring and security obligations, metadata and telemetry data can be processed, stored or transferred outside of the Union to the extent strictly necessary and proportionate to ensure the cybersecurity protection of the cloud computing service, if that purpose cannot be reasonably achieved by processing such data within the Union and provided that such processing, storage or transfer does not disrupt service continuity and/or degrade the service quality**;

(d) the personnel, including the personnel of the subcontractors which are involved in the provision of the audited service are Union citizens and where appropriate, the personnel must also have the necessary national security clearance issued by a Member State when handling classified information, as defined in Article 2, point (21), of Regulation (EU) 2021/697;

(e) the audited service obtains a European cybersecurity certificate of at least assurance level 'substantial' 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;

(f) the data generated by using the audited service are not used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country and are not transferred outside the Union in any case;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(g) the audited provider and the subcontractors– which are involved in the provision of the audited service are not subject to the control of a third country or a legal entity established in a third-country.**; or** by way of derogation to ~~this criterion, a cloud computing service provider and its subcontractors which are involved in the provision of the audited service that are subject to the control of a third country or a legal entity established in a third-country may be audited for Union assurance level 3~~**the first subparagraph,** where ~~the Commission has adopted an implementing act under Article 19. Where the Commission has adopted an implementing act under Article 19,~~ the audited provider and the subcontractors which are involved in the provision of the audited service ~~must also~~**are subject to the control of a third country or a legal entity established in a third-country, that third country has been identified as associated under Article 18 and the audited provider and the subcontractors which are involved in the provision of the audited service** demonstrate that the necessary legal, technical and organisational measures have been implemented to ensure that the:

i. control of the third country or the legal entity established in a third-country over the audited provider 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~~. The audited provider should allow for reasonable access to the code~~;

ii. access by a third country or by a legal entity established in a third-country to customer data is prevented;

iii. possibility of disruption of the service continuity and/or the degradation of the service quality by a third country or a legal entity established in a third country is prevented;

iv. ~~control of the third country or the legal entity established in a third-country over the audited provider 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;~~

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(ga) The cloud computing service provider supports standards-based integration of external identity providers for authentication and access management for the cloud service;

(gb) The cloud computing service provider provides customers with the capability to record, retain, and review logs of management and data access activities related to cloud service customer data. These logs should enable customers to identify when access occurred, the identity associated with the request, and the relevant operational context available through the service's logging capabilities;

(h) the technical and operational support or assistance related to the audited service, including subsequent sub-outsourcing arrangements, are initiated and performed exclusively within the Union, by personnel that are Union residents, and by third parties that are not subject to the control of a third country or a legal entity established in a third country;

(i) **where software is not released under an open source license,** the audited provider demonstrates that the following software supply chain measures are in place:

i. a complete and up-to-date SBOM and a list of identified dependencies relevant to the provision of the service are documented and made available to the auditing organisation;

ii. 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;

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

iii. where the cloud computing service provider is subject to the control of a third country or a legal entity established in a third-country, the cloud computing service provider ~~guarantees~~ **demonstrates** that there are no existing laws and practices in that third country, demonstrated by independent sources, that require the cloud computing service provider to report information on software vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(j) where software released under an open-source licence is used for the provision of the service, the audited provider demonstrates that it has 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;

(k) to the extent that the audited provider provides its services outside of the Union and maintains a subsidiary in a third country, the audited provider demonstrates that it has implemented the necessary measures to ensure and enforce the effective legal, technical and organisational separation between the Union parent company and any ~~such~~ third-country subsidiary.

3.2. ~~For Union assurance level 3, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship to the cloud computing service provider and that contribute to the provision and the delivery of the cloud computing service, and that may require access to classified or sensitive information, as defined in Article 2, point (22), of Regulation (EU) 2021/697.~~

4. Union assurance level 4

4.1. For Union assurance level 4, cloud computing service providers must meet the following cumulative criteria:

(a) the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

(b) the infrastructure, assets, and personnel of the audited provider, including the subcontractors , which are involved in the provision of the service, are located in the Union;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(c) the customer data, including metadata and telemetry data~~, which, following a risk assessment, is identified as sensitive~~, that is processed, stored and transferred by the audited provider and the subcontractors which are involved in the provision of the service, remain exclusively within the Union**, unless the Union entity, the contracting authority or the contracting entity explicitly allows otherwise,** and at any time, including before, during or after the configuration or use of the service;

(d) the personnel, including the personnel of the subcontractors-, which are involved in the provision of the audited service are Union citizens and, where appropriate, the personnel must also have the necessary national security clearance issued by a Member State when handling classified information;

(e) the audited service obtains a European cybersecurity certificate of ~~at least~~ assurance level '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;

(f) the data generated by using the audited service are not used to train or fine-tune any AI system operated by a third country or a legal entity established in a third-country, and are not transferred outside the Union in any case;

(g) the audited provider and the subcontractors which are involved in the provision of the audited service are not subject to the control of a third country or a legal entity established in a third-country;

(h) the technical and operational support or assistance related to the audited service, including subsequent sub-outsourcing arrangements, are initiated and performed exclusively within the Union, by personnel that are Union residents, and by third parties that are not subject to the control of a third country or a legal entity established in a third country;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(ha) The cloud computing service provider supports standards-based integration of external identity providers for authentication and access management for the cloud service;

(hb) The cloud computing service provider provides customers with the capability to record, retain, and review logs of management and data access activities related to cloud service customer data. These logs should enable customers to identify when access occurred, the identity associated with the request, and the relevant operational context available through the service's logging capabilities;

(i) **where software is not released under an open source license,** the audited provider demonstrates that the following software supply chain measures are in place:

i. a complete and up-to-date SBOM and a list of identified dependencies relevant to the provision of the service are documented and made available to the auditing organisation;

ii. measures in place to 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;

(j) ~~where software released under an open-source licence is used,~~ the audited provider demonstrates that it has 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;

(k) to the extent that the audited provider provides its services outside of the Union and maintains a subsidiary in a third country, the audited provider demonstrates that it has implemented the necessary measures to ensure and enforce the effective legal, technical and organisational separation between the Union parent company and any such third-country subsidiary.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

4.2. ~~For Union assurance level 4, the subcontractors referred to in the first paragraph must be subcontractors that are third parties that have a direct contractual relationship to the cloud computing service provider, that contribute to the provision and delivery of the cloud computing service, and that may require access to classified or sensitive information in order to carry out the service provision.~~

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

ANNEX III

Audit Evidence For The Audit Procedure

Auditing organisations should request the audit evidence listed in this Annex from the audited provider when assessing the compliance of the audited service against the applicable audit criteria under Annex II.

This Annex is indicative**, not exhaustive,** and does not limit the evidence that may be requested or considered by the auditing organisations. Auditors may seek any additional information necessary to ensure a comprehensive and accurate assessment of compliance **and** 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. **When undergoing independent third-party audits, audited providers can reuse existing evidence, including evidence used from previous audits referred to in Article 20 paragraph 1, valid certificates, evidence from other audits, conformity assessments or any other evidence issued under applicable Union or national law to the extent that such evidence demonstrates compliance with the relevant audit criteria under Annex II. The auditing organisation should take into account such evidence for the purpose of the audits.**

1. Audit criterion A – Union establishment

   The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (a) of Annex II based on the following:

(1) Any evidence demonstrating that the audited provider is incorporated under the law of a Member State in the Union or otherwise constituted in line with company law of a Member State in the Union.

(2) Any evidence that the registered office, central administration, and main establishment of the audited provider is established within the Union.

(3) The auditing organisation should verify the applicable Union legal framework of the audited provider and verify whether their establishment is genuine and stable or whether the audited provider instead qualifies only as a non-EU provider offering services in the Union.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(4) The auditing organisation should verify whether the provider is legally incorporated in a Member State of the Union. Evidence of this could include, but is not limited to, the national company extracts, tax residency documentation, business licences, VAT registration, verification of whether the provider is registered in the Business Registers Interconnected System (BRIS) and the VAT information Exchange System (VIES).

(5) The auditing organisation should verify the stable and effective presence in the Union of the audited provider. The auditing organisation should therefore verify that:

(a) EU physical offices or operational premises exist (for example, through lease contracts, utility bills or property documents);

(b) permanent staff is located in the Union and that customer support operations are carried out in the Union (for example, through **samples of** employment contracts~~, payroll records, personnel timesheets~~);

(c) contractual operations are handled in the Union (for example, through activity management records, incident reporting records);

(d) banking and accounting functions are exclusively in the Union (for example, through financial statements and statutory audit reports).

(6) The auditing organisation should verify the presence of EU Member State establishment units or branches (for example, through lease contracts, utility bills, property documents~~, employment contracts, timesheets, payroll records or purchase orders~~).

2. Audit criterion B – Location of infrastructure, assets, and personnel

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (b) of Annex II based on the following evidence:

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(1) Location of infrastructure

(a) A list with relevant details of the location of the infrastructure and data storage locations used in the provision of the audited service. This list should include the ~~precise~~ location ~~(number, street, city, postal code and country)~~ of the infrastructure demonstrating that all elements remain within the Union for the provision of the audited service. **The audited provider shall present the structure of its infrastructure (e.g. region, realm, availability zone) and the repartition between those it owns and those rented.** This includes the location for the primary, backup, disaster recovery and log storage.

(b) Any other evidence that the IT infrastructure is located in the Union such as lease agreements, property deeds, maintenance contracts, service contracts, facility access logs.

(c) Network diagrams and architecture documents illustrating the exclusive use of Union-based infrastructure for data storage and processing, including backup and replicated data.

(ca) A list with relevant details of implemented security perimeters measures, including the various means of access restriction and access control to zone supporting the audited service.

(2) Location of assets

(a) A list and relevant details of the assets used in the provision of the audited service, such as an asset register.

(b) Evidence that servers, equipment, and operational assets are located in the Union, such as records identifying the server and its location, purchase invoices, delivery notes, licence agreements, subscription contracts, or invoices for software purchases or subscriptions, invoices with delivery proofs for hardware.

(c) Evidence that service delivery capabilities are based in the Union, such as deployment records, installation records, service status reports, configuration reports, monitoring outputs, admin logs showing usage of the service.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(3) Location of personnel

(a) A list and relevant details of the personnel involved in the provision of the audited service.

(b) Evidence that the personnel involved in the provision of the audited service are located in the Union, including employment contracts, payroll records, timesheets, activity records, and organisational charts showing Union-based staff with operational responsibilities.

(4) Considerations regarding the infrastructure, assets and personnel

(a) The auditing organisation should also assess where such infrastructure, assets, or personnel:

i. store, transmit, access, process or otherwise handle customer data;

ii. provide, enable, or could enable administrative access to, control over, configuration of, or visibility into customer data;

iii. if compromised, misconfigured, made unavailable or disrupted could reasonably result in the disruption or unavailability of the audited service.

~~NB: 'Infrastructure' means physical infrastructure, including but not limited to, data centre infrastructure or colocation infrastructure, network, cooling, and IT systems that allow for the management of the datacentre.~~

~~'Assets' means hardware and software, including, but not limited to, libraries, the internal network needed for software components to communicate, cryptographic materials that enables the provision of the cloud computing service.~~

~~'Personnel', including personnel managed by subcontractors, means individuals who support the delivery, administration, security, availability, or operation of the audited service.~~

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

3. Audit criterion C – Data localisation in the Union

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (c) of Annex II based on the following evidence:

(1) Evidence demonstrating that customer data are stored and processed exclusively in the Union and that third-parties or subcontractors that do not meet the conditions under this Annex are in no circumstances technically or operationally able to access, obtain, make unavailable, destroy or more generally process customer data without prior authorisation. Examples include access logs, support access policies, privileged access records, backup retention policy, data flows diagram demonstrating where the customer data are stored, processed, replicated and backed up. When processing personal data, contracts with the subcontractors that demonstrate compliance with Regulation (EU) 2016/679.

(2) Evidence of logs and monitoring records demonstrating that all data are stored and processed exclusively within the Union. Examples include master service agreements, data processing agreements, data residency contractual agreements or any EU data boundary.

(3) Evidence (such as contractual agreements, logs, and procedures offered to public sector bodies) demonstrating that the audited provider and the subcontractors which are involved in the provision of the audited service have put in place the necessary measures to ensure that:

(a) no customer data, including encrypted data, are transferred outside of the Union without public sector body approval;

(b) no data are transferred to any third-party other than subcontractors which are involved in the provision of the service or recipients expressly authorised by the public sector body.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(4) A data flow diagram showing the flows of data between the cloud computing service provider and customer data, as well as with third-party services and subcontractors. The diagram must clearly identify the source and destination of data and demonstrate that the data does not leave the Union.

Evidence demonstrating the audited organization has established a service agreement with each of its customers entities of the service.

~~NB: For the purpose of this Annex, a customer means a public sector body who has entered into a contractual or other legally binding arrangement with the cloud computing service provider for the purpose of accessing or using the cloud computing service.~~

~~'Customer data' could mean any data under the control of the cloud computing service 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 compunting 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.~~

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

4. Audit criterion D – Union citizenship

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (d) of Annex II based on the following evidence:

(1) The audited provider should provide the auditing organisation with proof that it has implemented the measures to ensure that, if a public sector body were to request Union citizenship, the personnel involved in the provision of the audited service are Union citizens. This can be demonstrated through **providing a list of personnel and their nationalities which is subject to sample checks by the auditing organisation. This can be further checked through** valid official government issued documents (e.g. valid passport and national identity card);

(2) The audited provider should provide organisational charts and job descriptions confirming that it can ensure, where requested, that only personnel with Union citizenship have access to the audited service's operation, management, maintenance, and support.

(3) The audited provider should provide documents demonstrating access control policies and audit trails showing that only authorised personnel who are Union citizens can access the service's systems and data.

(4) The audited provider should demonstrate that it has put in place procedures describing how citizenship is verified before assignment and how compliance with this audit criterion is maintained throughout employment.

NB: Personnel involved in the provision of the audited service could include personnel who have logical or physical access to infrastructure and assets used to operate the cloud computing service, as well as those who are responsible for customer support, and all personnel who have management control of the cloud computing service provider.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

5. Audit criteria E – European cybersecurity certification scheme adopted under Regulation 2019/881

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (e) of Annex II based on the following evidence:

(1) A valid European cybersecurity certificate issued by a competent conformity assessment body demonstrating that the audited service has been assessed and found compliant with the requirements corresponding to the 'basic', 'substantial' or 'high' assurance levels under a European cybersecurity certification scheme adopted under Regulation (EU) 2019/881, provided that such shas been established ;

(2) A certification report including a description of the main components used for the development and operation of the cloud computing service that is covered by the audit certificate.

(3) Until the European cybersecurity certification scheme covering cloud computing services has been established, the audited provider can demonstrate compliance through valid cybersecurity certifications. This can include, but is not limited to, the following:

(a) a valid certificate issued by a competent conformity assessment body (in line with CEN/CLC/TS 18072:2025) demonstrating that the cloud computing service has been assessed and found compliant with the requirements corresponding to the 'basic' or 'substantial' or 'high' assurance levels defined under CEN/TS 18026:2024;

(b) A valid certificate issued ~~by the relevant~~ **under the** national **cybersecurity certification scheme in place in the Member State by the body** competent ~~authority~~ **to issue it under that scheme,** demonstrating that the cloud computing service has been assessed and found compliant with the requirements under the national cybersecurity scheme currently in place in the Member State;

(c) in the absence of a national scheme, evidence demonstrating adherence to the highest level of cybersecurity standards available on the market.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

6. Audit criterion F – AI systems operated by a third country or third country legal entity

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (f) of Annex II based on the following evidence:

(1) Contractual clauses stating that data processed or generated by using the audited service, including customer-derived data, logs and telemetry, will not be used to train or fine-tune any AI model or system operated by a third country or a third-country legal entity, and are not transferred outside the Union in any case.

(2) Contractual clauses specifying that data are processed solely for the delivery of the audited service and not for service improvements or model or system enhancements or any other secondary purpose.

(3) Data flow diagrams documenting the end-to-end flow of data, covering data ingestion, storage, processing ~~and~~**,** deletion **and data protection mechanisms**. The diagrams should also show where the AI pipelines or machine learning operations (MLOps) connect with customer data.

(4) MLOps or deployment records demonstrating that the build, test and release locations are in the EU.

(5) Model or system cards covering the model or system name, version, training and validation sources, including statements that the data generated by using the audited service does not leave the Union.

(6) Data lineage polices and related implementation documentation that shows that the provider operates data lineage and provenance tools and that can demonstrate (per record) what the data has been used for.

(7) A list of the subcontractors (indicating their country of establishment) that access the data generated by using the audited service.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

7. Audit criterion G – Absence of third-country control or third-country entity control

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (g) of Annex II based on the following evidence:

(1) **The audited provider must provide to** the auditing organisation ~~should identify and analyse~~:

(a) all direct and indirect shareholders, up to the ultimate owners **and clearly identify State-owned shareholders and those related to a third country**;

(b) the cap table documenting the company's ownership structure;

(c) the body or bodies empowered to take strategic decisions (general assembly of shareholders, supervisory board, board of directors, etc.) **and a governance scheme of its organisation**;

(d) the rules for the appointment/election/removal of governing bodies and the actual composition of the governing bodies (e.g. to identify if any shareholder is entitled to nominate a board representative or has majority seats in the board) **and the measures taken by the audited provider's governance to list non-EU legal and regulatory requirements that may apply to the service**;

(e) the quorums and majority required for adopting strategic decisions, in order to determine if any shareholder can take a strategic decision (either because they have the required majority to approve such a decision or because they can block such a decision through a veto or other specific rights even if they cannot impose such a decision on their own, etc.);

(f) the possible influence on strategic decisions through commercial links, financial links or other means, **the audited provider's strategic contracts that could expose it to the influence of third countries, and specify the mitigation measures to address this** etc.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(2) The audited provider should request all the above information from its subcontractors and make it available to the auditing organisation. **The audited provider must also document - from among its directly involved subcontractors - those likely to be exposed to the influence of third countries and legal entities established in third countries, and must specify the mitigation measures put in place to address this.**

7.1. Assessment of ownership and control:

(1) The audited provider should provide the auditing organisation with the following evidence related to the headquarters:

(a) the location and full address of the global headquarters and/or head office;

(b) the locations of the executive management structures.

(2) The audited provider should provide the auditing organisation with the following evidence related to the ownership structure and specific rights:

(a) A detailed list describing any owners that:

i. hold, directly or indirectly, at least 5% of the capital or at least 5% of the voting rights, including through any content, understanding, relationship or intermediary. This includes voting agreements between shareholders that would together have more than 5% of the voting rights or 5% of the capital;

ii. have one or more of the following specific rights in relation to their ownership: (a) right to veto a transfer of shares; (b) pre-emption rights; (c) right to purchase additional shares or investment subject to conditions.

(b) The auditing organisation should request the following supporting documents to assess the elements in paragraph 2(a):

i. commercial registry extracts and shareholders' books of the organisation and any other relevant document that clearly indicate the shareholders and their voting rights or percentage of interest;

Obtenu pour vous par
Obtained by
agence europe

Agence Europe

ii. shareholders' agreement, memorandum of understanding among shareholders, statutes, articles of association or other relevant documents regarding the decision-making procedures within the legal entity, investment agreements between the shareholders, etc.;

iii. for any shareholders that are legal persons that hold at least 5% in the capital or at least 5% of the voting rights:

(1) a graph describing the different ownership layers/chain of control until the ultimate owners;

(2) the articles of association, bylaws or equivalent constitutional documents;

(3) a register of directors, officers and signatories.

(3) The audited provider should provide the auditing organisation with the following evidence related to the corporate governance:

(a) The audited provider should provide the auditing organisation with a description of:

i. the decision-making bodies, their composition as well as their nationality or place of establishment (where applicable);

ii. the rules regarding election, appointment, nomination or tenure of members of the decision-making bodies or other management positions;

iii. the decision-making procedures, including information on the required majority and/or quorum needed for decisions;

iv. internal governance policies describing how ownership and control decisions are recorded and approved;

board and management decisions reflecting the stated control structure;

board minutes and resolutions for control changes.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(b) The audited provider should provide the auditing organisation with supporting documents setting out or describing: the decision-making bodies and the rules on their election, appointment, nomination or tenure, decision-making procedures, voting rights, veto rights, appointment rights, approval rights within the legal entity (e.g. articles of association bylaws, reports on corporate governance, etc.). The supporting documents and information should be provided for each intermediate legal entity that directly or indirectly holds 5% or more of the capital or voting rights, up to the ultimate owners of all the layers involved.

(4) The audited provider should provide the following control-related evidence to the auditing organisation:

(a) The audited provider should provide the auditing organisation with the evidence of the commercial links conferring control. This includes, but is not limited to, a list of individuals or legal entities with whom the audited providers (or the owners of the audited provider, including intermediate layers until the ultimate owners) have a commercial relationship that (a) leads to a similar level of control on management and resources as the ownership of shares or assets; and (b) is of very long duration (e.g. very important long-term supply agreements or credits provided by software manufacturers/customers, coupled with structural links).

(b) The supporting documents should include cooperation agreements with the public sector body or software manufacturers , etc.

(5) The audited provider should provide the auditing organisation with the following evidence related to the financial links conferring control:

(a) The audited provider should list the individuals or legal entities (including controlling shareholders or owners) on whom the audited provider (or the owners) are financially dependent in a way that could allow them to obtain concessions in strategic business areas.

(b) The supporting documents should include loan documents, by-laws, documents showing the financial link; etc.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

(6) The audited provider should provide the auditing organisation with the following evidence related to other sources of control:

(a) The audited providers should indicate to the audited organisation if there is any other means, process or link ultimately conferring control to another third country or a legal entity established in a third country (similar level of control on management and resources as the ownership of shares or assets and of long duration).

(b) Supporting documents should provide evidence of any such control or a declaration that there is no such control (this declaration may come from the management board of the service provider).

NB: The elements that should be taken into account when assessing control are the ownership structures and specific rights, corporate governance, commercial links conferring control, financial links conferring control and any other sources of control.

7.2. Additional steps based on the conclusion of the ownership and control test

If the auditing organisation determines that the audited provider is subject to the control of a third country or a third-country legal entity, it should request the following additional evidence:

(a) ~~Demonstrating~~ **Where recognition at Union assurance level 3 is sought, the auditing organisation should check** that the Commission has adopted a decision pursuant to Article ~~19~~**18** regarding the third country for which the cloud computing service provider is subject to the control of;

(b) All evidence demonstrating that the audited provider and any subcontractor involved in the provision of the audited service has implemented the necessary measures to enforce the effective legal, technical and organisational separation between the cloud computing service provider and any third country or legal entity established in a third country, ensuring that the cloud computing service provider is unable to comply, legally, technically and operationally, with any request to access customer data, including encrypted data, or to disrupt service continuity or to degrade service quality.

(c) All evidence demonstrating that the public sector body will be informed of any such request and a confirmation that the request has been refused;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(d) All evidence demonstrating the maintenance of an up-to-date record of any request to access customer data, to disrupt service continuity or to degrade service quality from a third country or a legal entity established in a third country, containing at least the request and the response to the request.

8. Audit criterion H – No technical and operational support outside of the Union

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (h) of Annex II based on the following evidence:

(1) evidence that the audited provider has implemented binding contractual clauses stating that all support, administration, maintenance, monitoring, incident response, and operational activities must be initiated and performed exclusively in the Union. This could include contractual clauses requiring advanced disclosure of all subcontractors and support locations, prior written approval before engaging any new subcontractors, and a right to reject any subcontractors located outside of the Union;

(2) evidence that the audited provider maintains an up-to-date subcontractor register**. The audited provider must provide a list of the involved subcontractors (indicating their country of establishment) that deliver technical and operational support. Providers should also specify whether their subcontractors further subcontract services related to the audited service**;

(3) evidence that the audited provider does not subcontract or transfer such activities outside of the Union;

(4) evidence that the audited provider has implemented the necessary legal, technical and organisational measures to ensure that there can be no remote access for technical and operational support from outside the Union for the audited service.

(5) evidence that the audited provider's help desk/support services, infrastructure administration, operations of its security operations centre (SOC) or network operations centre (NOC), privileged access, backup handling, and disaster recovery operations of the audited service are exclusively provided from the Union, including the access path to operate the service;

(6) evidence that the audited provider ensures that the personnel upon the departure from the company have no further access to the audited service and revokes all access policies;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(7) evidence that the audited provider has implemented the necessary technical and organisational measures to ensure that administrative access to systems used to operate the audited service is provided through access paths located within the Union. This can be demonstrated through the implementation of geographically restricted network controls, Union-based administrative infrastructure, privileged access management controls, and monitoring mechanisms;

(8) ~~evidence that the audited provider has procedures in place that there is no effective control of a third country or a legal entity established in a third country, including for subsequent sub-outsourcing.~~

9. Audit criterion I - Ensuring the transparency of the software supply chain

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (i) of Annex II based on the following evidence:

(1) The audited provider should make available to the auditing organisation a complete and up-to-date software bill of materials (SBOM) for all software components, including open-source software (OSS).

(2) The audited provider should make available to the auditing organisation a list of dependencies. This should include:

(a) all software modules, libraries or application programming interfaces (APIs) used, as well as development tools;

(b) origin of software: where (country of origin) and by whom the software is designed, developed and maintained, the location and jurisdiction governing the software distribution, and updates;

(c) degree of reliance on non-EU vendors, facilities, or proprietary technologies; for level 3, evidence that in case the software stack is provided by a third ~~country~~ **country** entity, no ~~unduly~~ unjustified licensing restrictions are in place.

(d) degree of reliance on open-source software;

(e) visibility into the entire software manufacturer and sub-manufacturer chain, including audit rights.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

N.B. The requirements above imply that joint ventures made, e.g., of a Union entity with a legal entity established in a third country can qualify for this level

(3) The audited provider should provide:

(a) evidence of a risk-based process for identifying and mitigating dependencies on external software manufacturers relevant to the operation of the cloud computing service;

(b) **where technically and operationally feasible,** evidence ~~that it has identified~~ **identifying** one or more **reasonable** alternative software solutions, including open-source software. ~~If~~ **Where** equivalent software cannot be identified, a solution ensuring minimal viable functionality must be identified. ~~Tests~~ **Contingency procedures** must be ~~implemented and a switchover plan enabling migration to such alternative solutions;~~ **documented and maintained in a manner proportionate to the role, criticality and replaceability of the software component concerned.**

(c) evidence that ~~it can migrate to an alternative solution in the event of any defect or~~ **contingency procedures exist for software dependencies and that the risks associated with vendor** failure ~~of the vendor~~ or restrictions ~~from~~ **imposed by** a third country or a legal entity established in a third country **have been assessed and documented**;

(d) provide a list of open standards that are followed as part of the audited providers policies regarding the audited service;

(4) The audited provider should ensure transparency through remote access and source code auditability by:

(a) making available to the auditing organisation a list of evidence to prove 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. This should include:

i. evidence related to the testing of the software component 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 (test procedure, test reports, test plan, etc.);

Agence Europe

Obtenu pour vous par
Obtained by
agence europe

ii. evidence that the organisation's change management procedures cover any change in firmware, bios and software updates as well as integration of a new components to prevent the use of any remote feature or mechanism;

iii. evidence that the maintenance procedure is updated to include preventing any remote feature or mechanism that could be used to materially tamper with or disrupt a device, system or software.

(b) The audited provider must ensure that the third-party independent auditor is granted the right to access and audit the source code of such software. The audited provider must also ensure that all documentation, technical material, information necessary to evaluate and audit the source code are made available to the auditing organisation in a complete, accurate, and accessible format.

10. Audit criterion J – Open-source software

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (j) of Annex II based on the following evidence:

(1) The audited provider should ensure transparency through remote access and source code auditability by:

(a) making available to the auditing organisation a list of evidence to prove 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. This should include:

i. evidence related to the testing of the software component 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 (test procedure, test reports, test plan, etc.);

ii. evidence that the organisation's change management procedures include any change in firmware, bios and software updates as well as integration of new components to prevent the use of any remote feature or mechanism;

iii. evidence that the maintenance procedure is updated to include preventing any remote feature or mechanism that could be used to materially tamper with or disrupt a device, system or software;

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(2) The audited provider should provide:

(a) evidence of a risk-based process to identify and mitigate: (i) a weak ecosystem and community support of the OSS; (ii) a failure to continuously monitor the updates released; (iii) cases where the OSS is deprecated or is no longer maintained.

(b) evidence that ~~the audited provider has~~ **security-relevant updates to open-source software are assessed and** applied ~~the up-to-date OSS~~ without undue delay**, taking account of vulnerability severity, compatibility, operational stability and the risks associated with the update itself**;

(c) evidence that the audited provider has identified one or several alternative open-source solutions. If the audited provider cannot identify an equivalent software, it must identify a solution ensuring minimal viable functionality. The audited provider must implement tests must and a switchover plan enabling migration to the alternative solutions.

(3) Where ~~the audited provider uses software released under an~~ open-source ~~licence~~ **software is used for the provision of the audited service**, the audited provider should ~~implement mechanisms to detect and~~ **monitor material changes in the governance, maintenance, distribution channels, signing infrastructure or security support of the open-source project and assess whether such changes materially affect the risk profile of the audited service. Where such changes materially affect the risk profile, the audited provider should** provide timely notice to the ~~public sector body if the software is acquired by or comes under control of a third country or a legal~~ **Union entity, the contracting authority or the contracting** entity ~~or foundation established in a third country~~.

11. Audit criterion K – Global services and subsidiaries in third-countries

The auditing organisation should assess the audit criterion listed under Union assurance levels 2, 3, and 4 paragraph (k) of Annex II based on the following evidence:

(1) The auditing organisation should verify that ~~the subsidiary is legally and operationally independent from~~ **effective legal, technical and organisational separation is maintained between** the audited provider **and the third-country subsidiary in accordance with Annex II**.

Obtenu pour vous par
Obtained by
agence europe
Agence Europe

(2) The audited provider must demonstrate that the subsidiary has no access to systems processing or storing the customer data.

(3) The audited provider must demonstrate that the subsidiary has no privileged accounts within the Union production environments, including cloud administration, Identity and Access Management (IAM), Privileged Access Management (PAM), monitoring or database administration privileges.

(4) The auditing organisation should verify that the personnel of the subsidiary cannot obtain access to Union customer data.

(5) The auditing organisation should verify that the subsidiary has no authority to instruct Union operational staff to disclose **Union** customer data or bypass **Union** security procedures.

(6) The auditing organisation should verify that all foreign government requests **concerning Union public sector bodies and** received by the subsidiary are formally redirected to the competent Union entity for legal assessment under Union and Member State law.

Agence Europe

Obtenu pour vous par
Obtained by
agence europe