EUROSMART
The Voice of the Digital Security Industry

Making CADA Deliver: Trust, Sovereignty and Competitiveness for Europe's Cloud and AI Future

Eurosmart Position Paper on the Cloud and AI Development Act (CADA)

Executive Summary

Eurosmart, the voice of the cybersecurity industry in Europe, welcomes the Cloud and AI Development Act (CADA) as an important step towards strengthening Europe's digital sovereignty, fostering a competitive and innovative cloud and AI ecosystem, and reducing strategic dependencies in critical digital infrastructure.

The proposal introduces a comprehensive set of measures intended to strengthen Europe's cloud and AI ecosystem. These include the establishment of the Union Cloud Sovereignty Framework, complementing the EU Cloud Services (EUCS) certification scheme, initiatives supporting the deployment of cloud and AI infrastructure, procurement mechanisms promoting European added value, and measures designed to enhance the Union's technological resilience.

Eurosmart strongly supports the overall objectives of the proposal. However, several aspects of the framework could be further strengthened to improve trust, legal certainty, consistency of implementation, market uptake and SME participation.

Eurosmart recommends measures to strengthen trust and consistency in the Union Cloud Sovereignty Framework (Amendments 1, 2, 3, 5, 6 and 7), preserve the integrity of sovereignty assurance levels (Amendments 4, 9 and 15), improve governance and regulatory maintenance (Amendments 8, 12, 13 and 17), increase practical adoption of the framework (Amendments 10 and 11), strengthen SME participation in cloud and AI procurement (Amendments 16–20), and safeguard the sovereignty objectives underpinning common procurement mechanisms (Amendment 14).

1. Strengthen Trust and Consistency

Trust is fundamental to the uptake of the Union Cloud Sovereignty Framework. Public authorities, but also operators of essential services and private-sector organisations must be able to rely on recognition solutions that are based on robust, consistent and comparable assessment methodologies across the Union.

Eurosmart therefore supports **the introduction of accreditation and competence requirements for auditing organisations** (Amendments 1 and 6). Recognition decisions under the framework rely heavily on independent assessments. Ensuring that auditing organisations possess appropriate technical expertise, independence and organisational capacity would strengthen confidence in assessment outcomes and promote consistent implementation across Member States.

Eurosmart also supports the **introduction of harmonised standards common specifications** and guidelines (Amendment 7). Without a common technical interpretation framework, similar cloud services could be assessed differently depending on the auditing organisation or Member State involved.

In addition, Eurosmart supports enabling the reuse of evidence generated through European cybersecurity certification schemes, including EUCS (Amendment 2). Cybersecurity certification schemes and sovereignty assessments pursue different objectives but often rely on overlapping technical and organisational evidence.

Finally, Eurosmart supports the introduction of **periodic reassessment mechanisms for recognised services and third-country recognition decisions** (Amendments 3 and 5). Recognition should remain subject to regular review to ensure that changes in ownership structures, governance arrangements, supply chains or geopolitical circumstances do not undermine compliance with the objectives of the framework.

2. Preserve the Integrity of Sovereignty Assurance Levels

The credibility of the Union Cloud Sovereignty Framework depends on the integrity of its assurance levels. These levels must provide clear and meaningful information regarding sovereignty safeguards, strategic autonomy and exposure to foreign control.

Eurosmart believes that Union **Assurance Level 3 should remain a distinct sovereignty assurance level** reserved for providers meeting enhanced sovereignty requirements (Amendment 4). Allowing cloud providers subject to third-country control to qualify for this level risks blurring the distinction between assurance levels and weakening confidence in the framework.

Eurosmart also supports strengthening **data localisation requirements for Union Assurance Levels 2 and 3 by removing possible derogations** allowing customer data to leave the Union (Amendment 15). Data localisation constitutes a core component of sovereignty assurance and contributes to continuity of service, strategic autonomy and protection against unlawful access to data.

Furthermore, sovereignty assurances must remain valid throughout the lifecycle of recognised services. Eurosmart therefore supports **ongoing surveillance audits and reassessment mechanisms** (Amendment 9). Recognition should not be viewed as a one-off exercise. Changes

in ownership, governance, subcontracting arrangements or operational infrastructure may materially affect compliance and should therefore be monitored on an ongoing basis.

3. Improve Governance and Regulatory Maintenance

Given the rapid evolution of cloud technologies, software supply chains, cybersecurity threats and artificial intelligence, the framework requires governance mechanisms capable of ensuring both consistent implementation and continuous adaptation.

Eurosmart supports the establishment of a **EuroCloud Coordination Group** (European Commission's expert group) (Amendment 12). Such a structure would provide a permanent forum for cooperation between the Commission, Member States, competent authorities, cloud service providers, users and other stakeholders. It would facilitate information exchange, support implementation and help ensure a common understanding of the framework's requirements.

Eurosmart also supports the introduction of a **structured review process for Annexes II and III** (Amendment 8). The technical requirements underpinning the framework must remain aligned with technological developments and emerging risks. Regular review cycles would ensure that the framework remains relevant and effective over time.

Enhanced monitoring and reporting obligations should also be introduced (Amendment 13). Effective implementation requires reliable information regarding procurement practices, use of assurance levels and the practical operation of the framework. Improved reporting would support evidence-based policymaking and facilitate future regulatory improvements.

4. Increase Adoption and Practical Use

The success of the Union Cloud Sovereignty Framework will ultimately depend on its practical adoption by organisations across the European economy.

Eurosmart supports strengthening the link between **the framework and the risk-management obligations established under the NIS2 Directive** through the introduction of **mandatory sovereignty-related impact assessments** and **the use of cloud computing services recognised at Union Assurance Level 3 or Union Assurance Level 4** for entities operating in sectors of high criticality (Amendment 10). Organisations increasingly rely on cloud services to support essential functions, making it important to assess risks relating to strategic dependencies, foreign control and operational resilience.

The proposal does not explicitly address **how private entities may rely on recognised cloud computing services**: the voluntary use of the framework by private organisations sould be claried.The Commission should also be empowered to develop guidance, methodologies and best-practice documents supporting implementation (Amendments 10 and 11). Clear guidance will be essential to ensure consistent application of the framework and facilitate its uptake across different sectors.

5. Strengthen SME Access to Cloud and AI Procurement

Innovative SMEs, start-ups and scale-ups are essential to Europe's cloud and AI ecosystem. Public procurement can play an important role in supporting their growth, strengthening competition and reducing excessive market concentration.

Eurosmart therefore supports increasing the target for procurement **awarded to innovative SMEs from 25% to 35%** (Amendment 16). A higher target would send a stronger signal to public buyers and help ensure that public spending contributes to the development of a diverse and innovative European technology ecosystem.

However, targets alone are not sufficient. Eurosmart supports the involvement of national **SME Envoys in monitoring implementation and identifying barriers faced by SMEs** (Amendment 17). Structured feedback from SME ecosystems can help improve procurement practices and ensure that policy objectives translate into tangible outcomes.

Eurosmart also supports the establishment of a **European SME Procurement Excellence Programme** (Amendment 18). Many innovative SMEs face practical difficulties in understanding procurement rules, identifying opportunities, preparing competitive tenders and scaling their activities to meet public-sector requirements. Training, guidance and capacity-building support would help address these challenges and improve participation in procurement markets.

To address barriers at the design stage of procurement procedures, Eurosmart supports the introduction of **an ex-ante SME Compliance Test** (Amendment 19). Contracting authorities should assess whether procurement requirements are proportionate and accessible before launching significant procurement procedures.

In addition, Eurosmart supports the formal involvement of national SME Envoys in monitoring SME participation in cloud and AI procurement procedures (Amendment 17). Their contribution would provide valuable insight into barriers affecting SME participation and strengthen implementation of the “Think Small First” principle.

Collectively, these measures would strengthen governance, improve coordination and support the long-term sustainability of the framework.

Finally, Eurosmart supports **making division into lots the default approach** for strategic or high-value cloud and AI procurement procedures, unless objectively justified otherwise (Amendment 20). This would create greater opportunities for SMEs and start-ups to participate in public procurement, strengthen competition and reduce structural market concentration.

6. Protect Sovereignty Objectives in Common Procurement

Common procurement can contribute significantly to the development of European cloud and AI capabilities and support the Union’s broader industrial and sovereignty objectives.

Eurosmart supports the introduction of **safeguards governing the participation of EFTA States and candidate countries in common procurement procedures** (Amendment 14). Participation should be based on reciprocity, equivalent obligations and demonstrable alignment with the objectives of the Union Cloud Sovereignty Framework.

Conclusion

Eurosmart strongly supports the objectives of the Cloud and AI Development Act and welcomes the establishment of a Union Cloud Sovereignty Framework as a key component of Europe’s digital sovereignty agenda.

The amendments identified in this paper would reinforce the effectiveness, credibility and practical value of the proposal. By strengthening trust and consistency (Amendments 1, 2, 3, 5, 6 and 7), preserving the integrity of sovereignty assurance levels (Amendments 4, 9 and 15), improving governance (Amendments 8, 12, 13 and 17), increasing practical adoption (Amendments 10 and 11), strengthening SME participation (Amendments 16–20) and safeguarding sovereignty objectives in procurement (Amendment 14), the Union can establish a framework that simultaneously advances competitiveness, innovation, resilience and digital sovereignty.

Summary of Recommendations

Strengthen Trust and Consistency

- **Amendments 1 and 6** - Require accreditation and competence requirements for auditing organisations.
- **Amendment 7** - Introduce harmonised standards and common specifications with presumption of conformity.
- **Amendment 2 -** Enable the reuse of evidence generated through EU cybersecurity certification schemes such as EUCS.
- **Amendments 3 and 5 -** Introduce a validity period for recognised services and periodic review of third-country recognition decisions.

Preserve the Integrity of Sovereignty Assurance Levels

- **Amendment 4 -** Maintain Union Assurance Level 3 as a distinct sovereignty assurance level by restricting third-country recognition to Union Assurance Levels 1 and 2.
- **Amendment 15 -** Remove derogations allowing customer data to leave the Union for Levels 2 and 3.
- **Amendment 9 -** Introduce ongoing surveillance and reassessment mechanisms for recognised services.

Improve Governance and Regulatory Maintenance

- **Amendment 12 -** Establish a EuroCloud Coordination Group to support implementation, stakeholder consultation and coordination.
- **Amendment 8 -** Create a structured review process for Annexes II and III.
- **Amendment 13 -** Improve monitoring and reporting obligations relating to procurement and implementation.
- **Amendment 17 -** Involve national SME Envoys in monitoring and assessment of SME participation in cloud and AI procurement.

Increase Adoption and Practical Use

- **Amendment 10 -** Strengthen the link between the framework and NIS2 risk-management practices.
- **Amendment 10 -** Introduce mandatory impact assessments for non-public entities operating in sectors of high criticality.
- **Amendment 11 -** Clarify that private-sector organisations may voluntarily rely on recognised cloud services.
- **Amendments 10 and 11** - Empower the Commission to issue guidance and best practices supporting implementation.

Strengthen SME Access to Cloud and AI Procurement

- **Amendment 16 -** Increase the target for procurement awarded to innovative SMEs from 25% to 35%.
- **Amendment 17 -** Create a structured feedback mechanism between SME ecosystems, national authorities and the Commission.
- **Amendment 18 -** Establish a European SME Procurement Excellence Programme to provide training, guidance and capacity-building support.
- **Amendment 19 -** Introduce an ex-ante SME Compliance Test to ensure procurement procedures are accessible, proportionate and SME-friendly.
- **Amendment 20 -** Make division into lots the default approach for strategic or high-value cloud and AI procurement procedures, unless duly justified.

Protect Sovereignty Objectives in Common Procurement

- **Amendment 14 -** Introduce safeguards governing the participation of EFTA States and candidate countries in common procurement procedures.
- **Amendment 14 -** Ensure reciprocity, equivalent obligations and alignment with Union sovereignty objectives.

#	Article	Original Text	Amendment	Rationale
1.	Article 2(17) - Auditing Organisations	'Auditing organisation' means an entity carrying out assessments under this Regulation."	**Add the following:** 'auditing organisation' means an entity accredited **by a national accreditation body designated pursuant to Regulation (EC) No 765/2008 and competent to carry out assessments under this Regulation."**	Ensures consistent competence and trust in audit outcomes across the Union.
2.	Article 16a - Relationship with cybersecurity certification schemes	No provision on reusing EUCS evidence	**New Article 16a** **Relationship with cybersecurity certification schemes** 1. Recognition under this Regulation shall be without prejudice to cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881. 2. Recognition under this Regulation shall neither require nor preclude certification under Regulation (EU) 2019/881. 3. Competent authorities and auditing organisations may take into account evidence generated through cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881, including audit reports, technical documentation, conformity assessment results, testing results and other relevant evidence, where	The Union Cloud Sovereignty Framework and cybersecurity certification schemes adopted under Regulation (EU) 2019/881 pursue distinct but complementary objectives Nevertheless, a significant portion of the technical, organisational and operational evidence generated through cybersecurity certification schemes may also be relevant for assessments carried out under this Regulation. Allowing competent authorities and auditing organisations to reuse such evidence helps reduce duplication, lower compliance costs and increase consistency between the two frameworks while preserving their distinct objectives.

#	Article	Original Text	Amendment	Rationale
			such evidence is relevant for the assessment of compliance with the requirements of this Regulation. 4. Where appropriate, competent authorities and auditing organisations shall seek to minimise duplication of assessments by reusing evidence already generated under cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881, provided that such evidence remains valid, reliable and relevant to the requirements being assessed.	
3.	Article 17 - Recognition of cloud computing service providers	Recognition granted to cloud computing service providers without defined validity period.	**Insert new paragraph: 17(15)** “Recognition granted under this Regulation shall remain valid for a period of three years. Providers seeking renewal shall submit an updated assessment demonstrating continued compliance with the applicable assurance level.”	Recognition should remain subject to periodic reassessment to ensure continued compliance with the requirements of the framework. Aligning the validity period with established certification practices provides legal certainty while ensuring that changes in ownership, governance, cloud architectures, supply chains or operational arrangements are periodically reviewed.
4.	Article 18(1) - Associated third countries	The Commission may adopt decisions, by means of implementing acts, identifying third countries for which cloud computing service providers subject to the	**Mofify Article 18(1):** “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	Union Assurance Levels 3 and 4 are intended to provide the highest degree of assurance regarding sovereignty, strategic autonomy and protection against foreign control. Allowing cloud service providers controlled from third countries to qualify for Union Assurance Level 3 risks undermining the distinction between

#	Article	Original Text	Amendment	Rationale
		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 the following cumulative criteria:	against the criteria for Union assurance **levels 1 and 2** pursuant to Annex II, provided that that third country fulfils the following cumulative criteria:"	the assurance levels and weakening confidence in the framework. Union Assurance Level 3 should remain a meaningful indicator of enhanced sovereignty assurances. Restricting access to Level 3 to providers satisfying the applicable ownership and control requirements preserves a clear distinction between the assurance levels and enables users to identify providers not subject to third-country control.
5.	Article 18 - Third-Country Recognition	Recognition procedure without periodic review.	**Add paragraph: (1b)** The Commission shall review recognition decisions adopted pursuant to this Article at least every three years and whenever significant legal, regulatory or geopolitical developments may affect compliance with the conditions set out in this Article. Where the Commission determines that a third country no longer fulfils one or more of those conditions, it shall amend, suspend or repeal the relevant recognition decision by means of an implementing act.	Third-country recognition decisions are based on legal, regulatory and geopolitical conditions that may evolve over time. Regular review is therefore necessary to ensure that recognised third countries continue to satisfy the requirements underpinning the Union Cloud Sovereignty Framework. The amendment also provides a mechanism for amending, suspending or withdrawing recognition where those conditions are no longer fulfilled, thereby preserving the credibility and effectiveness of the framework.

#	Article	Original Text	Amendment	Rationale
6.	New Article 21a - Accreditation and competence of auditing organisations	No clear provision for Auditing organisations	**New Article 21a** **Accreditation and competence of auditing organisations** 1. Auditing organisations carrying out assessments under this Regulation shall be accredited by the national accreditation body designated pursuant to Regulation (EC) No 765/2008. 2. Accreditation shall verify that the auditing organisation possesses the competence, independence, impartiality and organisational capacity necessary to perform assessments under this Regulation. 3. In particular, auditing organisations shall demonstrate competence in the assessment of: (a) cloud computing services, cloud architectures and cloud service management; (b) cybersecurity requirements, controls and certification schemes;	The framework relies extensively on independent audits to support recognition decisions, yet it does not establish accreditation or competence requirements for auditing organisations. This amendment ensures that assessments are carried out by competent, independent and impartial organisations, promotes consistent implementation across Member States and strengthens trust in the Union Assurance Levels.

#	Article	Original Text	Amendment	Rationale
			(c) data localisation, data governance and data access controls; (d) software supply-chain security, software dependency management and software bill of materials (SBOM) requirements; (e) operational resilience, business continuity and disaster recovery measures; (f) corporate ownership, governance and control structures; (g) AI governance requirements, including restrictions relating to the use of customer data for AI training and model development; (h) requirements relating to sovereignty, foreign control, strategic dependencies and lawful access to data. 4. Auditing organisations shall maintain personnel possessing the technical, legal and organisational expertise necessary to assess compliance with this Regulation, including the requirements set out in Annexes II and III.	

#	Article	Original Text	Amendment	Rationale
			5. The Commission may adopt implementing acts specifying accreditation criteria, competence requirements, audit methodologies, reporting templates and documentation requirements applicable to auditing organisations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article [X]. 6. The European Cloud Coordination Group shall facilitate the exchange of best practices concerning the accreditation, supervision and consistent assessment practices of auditing organisations. 7. Compliance with accreditation requirements under this Article shall be maintained throughout the period during which the auditing organisation carries out assessments under this Regulation. Where an auditing organisation no longer fulfils the requirements set out in this Article, it shall not perform assessments until compliance has been restored.	
7.	New Article 21b - Harmonised Standards and common specifications	Annex II is not backed to any kind of harmonised standards / common specifications to support the consistency of implementation	**New Article 21b** **Harmonised standards and common specifications**	Without harmonised standards / common specifications, the same cloud service could receive different audit outcomes depending on the auditing organisation or Member State conducting the assessment. The credibility of the Union Assurance Levels therefore requires

#	Article	Original Text	Amendment	Rationale
			1. Compliance with harmonised standards, or parts thereof, the references of which have been published in the Official Journal of the European Union, shall give rise to a presumption of conformity with the corresponding requirements of this Regulation covered by those standards. 2. The Commission may request one or more European standardisation organisations, in accordance with Regulation (EU) No 1025/2012, to draft harmonised standards supporting the implementation of this Regulation. 3. Where harmonised standards are unavailable, insufficient, or where delays in their development would adversely affect the effective implementation of this Regulation, the Commission may adopt common specifications by means of implementing acts. Compliance with such common specifications shall give rise to a presumption of conformity with the corresponding requirements of this Regulation. 4. Harmonised standards and common specifications may cover, inter alia: (a) software supply-chain transparency;	a common technical interpretation framework. The introduction of harmonised standards would provide a common technical baseline and a presumption of conformity mechanism similar to that found in other Union legislation, including the Cyber Resilience Act, the AI Act and the New Legislative Framework. The addition of common specifications would ensure that implementation is not delayed where standards are unavailable or insufficient.

#	Article	Original Text	Amendment	Rationale
			(b) software bill of materials (SBOM) requirements; (c) operational sovereignty controls; (d) data localisation and data residency controls; (e) verification of third-country ownership, control or influence; (f) cloud service portability and interoperability; (g) continuity of service and business continuity requirements; (h) audit methodologies and evidence requirements; (i) subcontracting and supply-chain management requirements; (j) logging, monitoring and traceability mechanisms relevant to sovereignty requirements. 5. When preparing requests for harmonised standards or common specifications, the Commission shall consult relevant stakeholders, including competent authorities, auditing organisations, cloud computing service providers, users,	

#	Article	Original Text	Amendment	Rationale
			standardisation organisations and the European Cloud Coordination Group.	
8.	New Article 21b - Review of Annexes	No provision for maintenaning the Annexes II and III	**New Article 21b** **Review and maintenance of Annexes II and III** 1. The Commission shall regularly assess whether Annexes II and III remain appropriate in light of technological developments, cybersecurity risks, cloud computing architectures, software supply-chain practices, AI systems and evolving sovereignty-related risks. 2. The Commission shall review Annexes II and III at least every three years. 3. In carrying out the review referred to in paragraph 2, the Commission shall consult: (a) the Eurocloud Coordination Group; (b) national competent authorities; (c) auditing organisations; (d) cloud computing service providers;	Annexes II and III contain the technical requirements underpinning the Union Cloud Sovereignty Framework. Given the rapid evolution of cloud computing, cybersecurity, software supply chains and AI technologies, those requirements should be subject to regular review. This amendment introduces a structured maintenance mechanism, stakeholder consultation process and review cycle to ensure that the framework remains effective, consistent and technologically up to date.

#	Article	Original Text	Amendment	Rationale
			(e) relevant standardisation organisations; (f) representatives of users, including public authorities, Essential Entities and private-sector stakeholders. 4. The Commission shall publish a report summarising the outcome of the review and identifying any elements requiring amendment. 5. Where appropriate, the Commission shall adopt delegated acts in accordance with Article [X] to amend Annexes II and III in order to reflect technological developments, emerging risks and internationally recognised standards.	
9.	Article 23a - Ongoing Compliance and Surveillance Audits	No mecanism to ensure compliance of cloud compiting service provider after recognition.	**New Article 23a** **Ongoing Compliance and Surveillance Audits** Providers recognised at Union Assurance Levels 3 and 4 shall undergo annual surveillance audits conducted by an accredited auditing organisation. The surveillance audit shall verify continued compliance with the requirements applicable to the relevant Union Assurance Level, including requirements relating to ownership, control, governance, operational resilience, data	Ensures ongoing compliance after recognition. Recognition is granted based on conditions that may evolve over time. Annual surveillance audits help ensure that changes in ownership, governance, infrastructure, subcontracting arrangements or operational practices do not undermine continued compliance with the applicable Union Assurance Level.

#	Article	Original Text	Amendment	Rationale
			localisation, software supply-chain security and sovereignty safeguards. Providers shall notify the competent authority without undue delay of any material change that may affect compliance with the requirements of this Regulation.”	
10.	Article 31 - Impact Assessments (Essential Entities)	NIS2 entities **may** perform assessments.	**Replace the article:** **Article 31** **Use of Recognised Cloud Computing Services by Essential Entities** 1. Entities referred to in Annex I of Directive (EU) 2022/2555 that are not public sector bodies and that procure cloud computing services supporting the provision of their essential services shall conduct an impact assessment in accordance with the methodology referred to in Article 29. 2. The impact assessment shall identify and evaluate risks relating to public order, continuity of service, strategic dependencies, foreign control, lawful access to data, operational resilience and other sovereignty-related risks associated with the use of cloud computing services. 3. Based on the outcome of the impact assessment, entities referred to in paragraph 1 that are not public sector bodies shall procure cloud computing	Non-public entities operating in sectors of high criticality increasingly rely on cloud computing services for the provision of essential services. Disruptions, strategic dependencies, foreign control, unlawful access to data or the loss of operational control affecting such services may have significant consequences for the security, resilience and continuity of critical societal and economic functions. This amendment strengthens the Commission proposal by introducing a mandatory impact assessment requirement for non-public entities operating in sectors of high criticality while preserving the Commission’s role in issuing guidance and adopting supplementary measures where necessary. It promotes a consistent approach to the assessment and mitigation of sovereignty-related risks and strengthens the link between the Union Cloud Sovereignty Framework and the risk-management obligations established under Directive (EU) 2022/2555. Given the critical nature of the services concerned, entities should rely on cloud computing services recognised at Union

#	Article	Original Text	Amendment	Rationale
			services recognised under this Regulation at Union Assurance Level 3 or Union Assurance Level 4 for services supporting the provision of their essential services, determining the appropriate assurance level in light of the nature, criticality and risk profile of the services concerned. 4. The Commission shall issue guidance on the methodology for carrying out the impact assessments referred to in this Article and on possible mitigation measures to be adopted by entities operating in sectors of high criticality. 5. Entities referred to in paragraph 1 shall review the impact assessment periodically and whenever a substantial modification is made to the cloud computing service, its provider, ownership structure, subcontracting arrangements or the functions supported by that service. 6. Where, because of specific circumstances, and where duly justified and in consultation with the Member States, the Commission concludes that additional impact assessment requirements or risk mitigation measures are necessary for entities operating in sectors of high criticality, it may adopt delegated acts in accordance with Article 45 supplementing this Regulation.	Assurance Level 3 or Union Assurance Level 4 when supporting the provision of essential services.

#	Article	Original Text	Amendment	Rationale
			7. The requirements set out in this Article shall be without prejudice to the obligations established under Directive (EU) 2022/2555 and other applicable Union sectoral legislation.	
11.	New Article 31a - Private Sector Use	No provision - Explicitly extend the use of recognised cloud computing services by private entities	**Article 31a** **Use of recognised cloud computing services by private entities** 1. Any natural or legal person may rely on the recognition of a cloud computing service under this Regulation when conducting risk assessments, procurement procedures, outsourcing arrangements, supplier due diligence, cloud sourcing decisions or compliance activities. 2. Private entities may take into account the Union Assurance Level attributed to a recognised cloud computing service when assessing risks relating to strategic dependencies, continuity of service, foreign control, lawful access to data, software supply-chain resilience and other sovereignty-related risks. 3. Recognition under this Regulation may be used as evidence that a cloud computing service has undergone an assessment against the requirements corresponding to	The proposal does not explicitly address how private entities may rely on recognised cloud computing services. This amendment clarifies the voluntary use of the framework by private organisations and enables the Commission to develop guidance supporting its consistent application in procurement, outsourcing, risk-management and compliance activities.

#	Article	Original Text	Amendment	Rationale
			the applicable Union Assurance Level. 4. Competent authorities and Union institutions may encourage the use of recognised cloud computing services in guidance, recommendations, procurement frameworks, risk-management methodologies and sector-specific best practices. 5. The Commission may issue guidelines, recommendations and best-practice documents concerning the use of recognised cloud computing services by private entities, including for the purposes of supply-chain risk management, outsourcing, operational resilience, cloud sourcing strategies, cybersecurity governance and compliance with Union legislation.	
12.	Article 31b - Expert Group	No provision for a stakeholders' expert group	**Article 31b** **EuroCloud Coordination Group** 1. A EuroCloud Coordination Group ('ECG') is hereby established. 2. The ECG shall support the consistent implementation of this Regulation and facilitate cooperation among the Commission, Member States, national competent authorities, auditing	The proposal establishes several complex and interdependent policy mechanisms, including Cloud and AI Leadership Initiatives, Data Centre Strategic Projects, the Union Cloud Sovereignty Framework, procurement requirements, the EuroCloud Federation and the Open Source Framework. However, it does not provide a permanent governance structure capable of supporting coherent implementation across these different chapters.

#	Article	Original Text	Amendment	Rationale
			organisations, cloud computing service providers, public authorities, users and other relevant stakeholders. 3. The ECG shall in particular: (a) facilitate the exchange of information, experience and best practices concerning the implementation of this Regulation; (b) contribute to the consistent interpretation and application of the requirements set out in Annex II and other technical requirements established under this Regulation; (c) support cooperation between national competent authorities in relation to recognition, supervision and enforcement activities under this Regulation; (d) identify emerging technological developments, market trends and sovereignty-related risks that may affect the effectiveness of this Regulation; (e) advise the Commission on the need to update Annex II, Annex III	The ECG would provide a structured stakeholder consultation mechanism and support coordination across the different components of the Regulation, including the maintenance of the annexes, thereby reducing the risk of fragmented implementation and improving the long-term effectiveness of the Union's cloud and AI policy framework.

#	Article	Original Text	Amendment	Rationale
			and other technical requirements established under this Regulation; (f) contribute to the development of guidance, model documentation, assessment methodologies and best practices for public authorities, Essential Entities and private users of recognised cloud computing services; (g) support the development of interoperability, portability and operational best practices among recognised cloud computing services; (h) contribute to the implementation of the Cloud and AI Leadership Initiatives established under Articles 3 and 4, including by identifying technological priorities, implementation challenges and opportunities for cooperation; (i) advise the Commission and Member States on the implementation of National Cloud and AI Strategies and the coordination of actions supporting strategic technology domains;	

#	Article	Original Text	Amendment	Rationale
			(j) contribute to the identification of future cloud, computing and AI infrastructure needs and support the monitoring activities established under Article 15; (k) provide recommendations concerning Data Centre Strategic Projects and the development of cloud and computing capacity within the Union; (l) support the implementation of Articles 32 and 33 by contributing to guidance and best practices relating to Union Added-Value Criteria and cloud and AI procurement; (m) facilitate cooperation and exchange of experience concerning the operation of the EuroCloud Federation established under Articles 34 to 36; (n) contribute to the development of best practices relating to open-source software reuse, interoperability, software sharing and cooperation between Open Source Programme Offices established under Articles 41 to 44;	

#	Article	Original Text	Amendment	Rationale
			(o) support stakeholder consultation and cooperation concerning the implementation and future development of this Regulation. 4. The Commission shall chair the ECG and provide its secretariat. 5. The Commission shall consult the ECG when preparing delegated acts, implementing acts, guidance documents, standardisation requests or common specifications under this Regulation.	
13.	Article 33 - Monitoring of procurement of innovation in cloud and AI	General monitoring obligation.	**Add new paragraph (1b):** Member States shall submit an annual report to the Commission on the implementation of Articles 29 to 32. The report shall include, where applicable, information on: (a) the use of Union Assurance Levels in procurement procedures; (b) the number and value of contracts awarded to recognised cloud computing services; (c) the application of Union added-value criteria;	The proposal uses procurement as a tool to support cloud sovereignty and industrial policy objectives, but does not establish clear indicators for measuring its effectiveness. Structured reporting and Commission evaluation would improve transparency, facilitate consistent implementation and enable evidence-based assessment of the framework's impact on procurement practices and the European cloud ecosystem.

#	Article	Original Text	Amendment	Rationale
			(d) the outcome of impact assessments carried out pursuant to Articles 29 and 31; and (e) any difficulties encountered in the implementation of this Regulation. The Commission shall publish a consolidated report assessing the implementation and effectiveness of this Chapter."	
14.	Article 38(9) - Participation of EFTA States and Candidate Countries	By way of derogation from Article 168(2) of Regulation (EU, Euratom) 2014/2509, 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 for such possibility.	**Replace Article 38(9) with:** Contracting authorities from EFTA States and Union candidate countries may participate in common procurement procedures under this Chapter only where such participation is provided for under an international agreement concluded with the Union. Such participation shall be subject to a prior assessment by the Commission demonstrating that: (a) the third country has adopted measures ensuring a level of protection equivalent to the requirements of this Regulation; (b) participation is consistent with the objectives of the Union Cloud Sovereignty Framework and the Union Added-Value Criteria established under this Regulation;	Common procurement is intended to support the development of European cloud and AI capacities and reduce strategic dependencies. Participation by EFTA States and candidate countries should therefore be based on a clear legal framework and subject to safeguards ensuring alignment with the objectives of the Regulation. The amendment preserves cooperation with closely associated European partners, ensure reciprocity, and protection of the Union's sovereignty and security interests.

#	Article	Original Text	Amendment	Rationale
			(c) participation does not adversely affect the strategic autonomy, security interests or sovereignty objectives of the Union. The Commission shall publish the assessment referred to in the second subparagraph. The international agreement shall ensure reciprocity and an equivalent level of obligations and safeguards to those applicable to Member States under this Regulation."	
15.	Annex II - Levels 2 and 3	"Customer data stored and processed in the Union unless the public authority explicitly requires otherwise."	**Delete:** "unless the public authority explicitly requires otherwise".	For Union Assurance Levels 2 and 3, data localisation constitutes a core element of the sovereignty guarantees provided by this Regulation. Allowing derogations from the requirement that customer data remain exclusively within the Union could undermine the objectives relating to continuity of service, protection against unlawful third-country access, strategic autonomy and public-order considerations. It is appropriate to require that customer data, including metadata and telemetry data, remain exclusively within the Union for cloud computing services recognised at Union Assurance Levels 2 and 3.
16.	Article 33 -	At least 25% of procurement for cloud computing services and AI	**Replace "25%" by "35%".**	A higher target would strengthen support for innovative SMEs and start-ups, improve access to public contracts, reduce market concentration and reinforce European

#	Article	Original Text	Amendment	Rationale
	SME Procurement Target	systems awarded to innovative SMEs.		technological capacity, resilience and sovereignty.
17.	Article 33(3)a (new) - SME Envoy Network	No provision requiring the involvement of national SME Envoys in the monitoring, assessment or reporting of SME participation in procurement procedures for cloud computing services and AI systems.	**Insert new paragraph 3a** "3a. Member States shall involve their national SME Envoy, designated within the SME Envoy Network, in the monitoring and assessment referred to in paragraphs 1 to 3. The national SME Envoy shall, in cooperation with the relevant national authorities and without prejudice to their respective competences, contribute to the yearly information submitted to the Commission pursuant to paragraph 3. The contribution shall include information on: (a) transparency and accessibility of procurement opportunities; (b) participation and success rates of SMEs, start-ups and small mid-cap enterprises; (c) structural, administrative, technical, financial or contractual barriers; (d) use of SME-friendly procurement strategies; (e) measures to improve SME access. Member States shall also ensure that their national SME Envoy contributes, where appropriate, to communication roadmaps, workshops and capacity-building initiatives.	The monitoring and reporting framework established under Article 33 would benefit from structured input from SME ecosystems and from a dedicated implementation channel at national level. National SME Envoys are well placed to provide practical insights into the barriers faced by SMEs, start-ups and small mid-cap enterprises when accessing procurement opportunities. This amendment strengthens the implementation of the "Think Small First" principle by establishing a structured feedback mechanism between SMEs, national authorities and the Commission. It improves transparency regarding participation and success rates, facilitates the identification of structural barriers and supports the development of targeted measures to improve SME access to procurement markets. It also promotes greater consistency in the assessment of Member States' progress towards SME participation objectives and contributes to more effective implementation of procurement policies supporting innovation, competition and technological sovereignty.

#	Article	Original Text	Amendment	Rationale
			The Commission shall take into account the contributions of national SME Envoys when assessing implementation of this Article."	
18.	Article 33(5)a (new) - European SME Procurement Excellence Programme	No dedicated Union-level programme providing training, guidance and capacity-building support to SMEs, start-ups and small mid-cap enterprises seeking to participate in procurement procedures for cloud computing services and AI systems.	**Insert new paragraph 5a:** "5a. The Commission shall, in cooperation with Member States, establish a European SME Procurement Excellence Programme to strengthen the ability of SMEs, start-ups and small mid-cap enterprises to access, participate in and successfully deliver public procurement contracts for cloud computing services and AI systems. The programme shall provide targeted training, workshops, practical guidance and capacity-building support and shall: (a) improve understanding of procurement rules; (b) support identification of procurement opportunities; (c) assist in preparing tenders; (d) support access to cross-border procurement; (e) strengthen delivery capacity; (f) disseminate best practices. The programme shall be deployed across the Union and implemented in coordination with SME Envoys, Enterprise Europe Network, chambers of commerce and other support structures. The Commission may develop a voluntary European SME Procurement Readiness Certification or	Improving SME participation in public procurement requires more than monitoring and reporting. Many innovative SMEs face practical challenges in understanding procurement rules, identifying opportunities, preparing competitive tenders and scaling their operations to deliver large public contracts, particularly in cross-border contexts. This amendment establishes a structured European SME Procurement Excellence Programme to strengthen procurement readiness and delivery capacity across the Union. By providing targeted training, workshops, practical guidance and capacity-building support, the programme would help SMEs compete more effectively in procurement markets, facilitate cross-border participation and improve access to public contracts. It would also contribute to strengthening European innovation ecosystems, promoting competition and ensuring that procurement policies support the growth and scaling of innovative European technology providers.

#	Article	Original Text	Amendment	Rationale
			Label.” .	
19.	Article 33(5)b (new) - SME Compliance Test	No mechanism requiring contracting authorities to assess, prior to launching a procurement procedure, whether procurement conditions are proportionate and accessible to SMEs, start-ups and small mid-cap enterprises.	**Insert new paragraph 5a:** “5b. For procurement procedures for cloud computing services and AI systems exceeding a strategic or financial threshold defined by the Member State or, where applicable, by the Commission, contracting authorities shall carry out an ex-ante SME Compliance Test before launching the procedure. The SME Compliance Test shall assess whether the procurement procedure has been designed in a manner that is accessible, proportionate and suitable for participation by SMEs, start-ups and small mid-cap enterprises. The Commission may issue guidance and templates for the SME Compliance Test to support consistent application across Member States and reduce administrative burden for contracting authorities.”	Monitoring SME participation after procurement procedures have been completed does not address barriers that may already be embedded in the design of those procedures. Requirements relating to contract size, qualification criteria, financial capacity, technical specifications or contractual conditions may unintentionally exclude SMEs from participation. This amendment introduces an ex-ante assessment mechanism requiring contracting authorities to consider SME accessibility at the design stage of procurement procedures. The SME Compliance Test promotes proportionate procurement practices, improves transparency, reduces unnecessary barriers to entry and encourages wider participation by innovative SMEs. It also supports competition, reduces market concentration and helps ensure that procurement frameworks contribute to the development of resilient and competitive European cloud and AI ecosystems.
20.	Article 33 (5)c (new) -	Division into lots is encouraged under existing procurement rules but is not required for	**Insert new paragraph 5c:** “5c. For procurement procedures exceeding a strategic or financial threshold, contracting	Large and highly integrated procurement procedures frequently create structural barriers that prevent SMEs, start-ups and small mid-cap enterprises from competing

#	Article	Original Text	Amendment	Rationale
	Mandatory division into lots	procurement procedures relating to cloud computing services and AI systems.	authorities shall divide contracts into lots, unless they provide a clear, written and verifiable justification explaining why such division would not be appropriate. The justification shall explain, where relevant, why division into lots would be technically impracticable or undermine interoperability, security, continuity of service or effective contract performance. Where contracts are divided into lots, contracting authorities shall design such lots in a manner that facilitates participation by SMEs, start-ups and small mid-cap enterprises.”	effectively, even where they offer innovative and specialised solutions. As a result, procurement markets may become concentrated around a limited number of large providers. This amendment establishes division into lots as the default approach for strategic or high-value procurement procedures while preserving flexibility where justified by technical, operational or security considerations. By facilitating participation in specific functional, technical, geographic or operational components of larger projects, the amendment promotes competition, reduces market concentration and creates greater opportunities for innovative SMEs to participate in public procurement. It thereby supports the development of resilient European value chains and strengthens the contribution of procurement policy to innovation, competitiveness and technological sovereignty.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com