EUROPEAN
COMMISSION

Brussels, 3.6.2026
COM(2026) 502 final

2026/0138 (COD)

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)

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

In recent years, cloud and AI technologies, services and applications have evolved from new concepts to indispensable pillars underpinning the functioning of our economy and society. AI unlocks unprecedented opportunities from automation and data-driven decision-making to personalised services, while cloud computing provides the computational resource, software building blocks and interfaces necessary for efficient AI development and deployment. The rapid proliferation of AI has resulted in an unprecedented and growing demand for computational capabilities. Consequently, computing infrastructures are no longer mere technical assets but have become strategic resources critical to the Union's economic security, sovereignty, resilience, and competitiveness.

As Mario Draghi's report 'The future of European competitiveness' states, the EU must maintain a foothold in areas where technological sovereignty is required, such as security and encryption ("sovereign cloud" solutions) and thus reduce critical external dependencies by strengthening homegrown cloud and AI capabilities and infrastructure. To this end, the Draghi report calls on the European Commission to take targeted actions aimed at regaining and retaining control over data and cloud computing services, expanding domestic computational capacity and establishing a robust financial and talent flywheel to drive innovation.

These objectives were later enshrined in the European AI Continent Action Plan, which presented a strategic roadmap to ensure European AI leadership. Central to achieving this is a nexus between five key domains: computing infrastructures, data, skills, development and adoption of AI algorithms, and regulatory simplification. The ongoing deployment of AI factories and AI gigafactories aims to provide broad access to high-capacity, next-generation computational resources for European businesses and researchers requiring AI capabilities. To complement this, the EU needs to expand its cloud and data centre capacity to support the wider deployment and diffusion of AI.

The Union's limited data centre capacity poses a significant threat to its ability to benefit from the digital transformation and adopt AI-driven solutions, notably those requiring low-latency compute capacity. In particular, several obstacles hinder the rapid deployment of data centres in the EU. As data storage and processing demands continue to rise - particularly due to the surge in AI workloads - the lack of data centre capacity in the EU forces European enterprises to route critical workloads through foreign hyperscaler infrastructure. This makes the EU a less attractive destination for tech investment than regions with more abundant, lower-cost compute resources.

The current landscape of cloud and AI is characterised by a **pronounced dependence on a limited pool of third-country providers**. While the EU market for cloud computing services market is growing significantly, the market share of EU providers decreased from 29% in 2017 to 15% in 2022 and has remained stagnant since then.

Currently, three non-EU hyperscalers control over 70% of the European cloud market. Large market incumbents are subject to third-country jurisdictions where laws with an extraterritorial effect apply, including laws mandating data access and transfer that may conflict with EU fundamental rights and data protection frameworks. This dependence also exposes European users to the risks related to operational discontinuity, particularly in scenarios where unilateral decisions by third-country actors could disrupt service provision.

Against this background, Europe has world-class research and development capabilities, vibrant open-source communities and a strong industrial base in cloud and AI, which however remain largely untapped.

Against this background, the Commission has prepared the **proposed Cloud and AI Development Act** ('the proposal') which aims to address the limited and geographically concentrated availability of computing capacity in the EU and the risks associated with dependence on cloud and AI supplied by non-European providers. The proposal aims to

(1) increase computing capacity and AI developed and deployed in the EU through innovative and sustainable Cloud and AI technologies;

(2) ensure attractive conditions for the deployment of sustainable and innovative computing capacity across the Union;

(3) address concerns regarding data sovereignty and operational continuity of cloud and AI;

(4) help protect public order by making the supply of cloud computing services more resilient, in particular in the public sector.

The proposal responds to the need for a coordinated 'ecosystem approach' to make the EU more competitive and resilient in the cloud and AI area. It combines supply-side measures to boost domestic capabilities, demand-side measures to drive adoption, and enablers to foster innovation and investment into cloud and AI. It places a specific focus on open source as a lever to boost technological sovereignty, in line with the EU Open Source Strategy which aims to promote open European alternatives across the European technology stack.

First, the proposal supports projects that are the outcome of the research and innovation initiative launched under this framework and implemented jointly with Member States. This initiative will integrate networks, cloud, AI and software into coherent ecosystems to address the following:

(1) future challenges across energy-efficient compute infrastructure;

(2) autonomy across the cloud stack;

(3) advanced EU capabilities in advanced AI technologies such as frontier AI, physical AI and industrial AI;

(4) adoption of cloud and AI across the public and private sectors.

The proposal places a particular emphasis on large-scale, cross-sectoral initiatives addressing the most strategic technological and industrial challenges ('grand challenges'). It will demonstrate the feasibility of this effort and pave the way for similar initiatives in the future, creating the conditions for investment in next-generation infrastructure and technologies.

Second, the proposal responds to the growing gap in data centre capacity with a framework that simplifies and harmonises the deployment of data centres EU-wide, while ensuring their sustainability. It aims to triple EU capacity in the next five-to-seven years and reach the needed capacity by 2035, while ensuring balanced geographic deployment across Member States. To support this, the proposal presents a mechanism to identify and support data centre strategic projects with significant built-in innovation and sustainability or that contribute to the balanced distribution of computing capacity.

Third, the proposal aims to mitigate the risks stemming from the EU's reliance on third countries for cloud computing services via a single EU-wide sovereignty framework. It provides a harmonised and auditable set of criteria at different levels of sovereignty of cloud

computing services. It also provides a framework for services to be assessed and formally recognised at a particular level of sovereignty. Finally, it obliges the Member States to undertake sovereignty risk assessments to determine which sub-sectors and use cases should be served by services aligned with the respective sovereignty levels to ensure appropriate protection in terms of data confidentiality, to ensure operational autonomy and to prevent harm that could undermine public order.

Complementing the **Cybersecurity Act (CSA2) revision**, which addresses supply chain risks, the proposal ensures that contracting authorities can use sovereign cloud computing services. Together, the proposal and the CSA2 fill long-standing gaps in sovereignty and non-technical risks. At the same time, cloud computing services in Europe must meet high cybersecurity standards, which calls for a robust cybersecurity framework that provides a comprehensive response to today's geopolitical security challenges. In this legislative context, work will resume on the **European Cybersecurity Certification Scheme for Cloud Services (EUCS)**.

The proposal finally provides a framework for contracting authorities to make informed purchasing decisions and leverage their buying power towards lowering existing dependencies, including through the use of sector-specific EU-added-value award criteria and common procurement to drive innovation and growth, with a focus on creating concrete opportunities for smaller EU-based providers.

Taken together, the measures set out in the proposal establish the foundations for a resilient, high-performance EU cloud and AI ecosystem. They position Europe not just as a consumer of advanced digital technologies but as a global hub for trusted, sovereign and scalable digital infrastructure capable of shaping the standards, capabilities and markets of the next technological wave.

- **Consistency with existing policy provisions in the policy area**

The proposal is consistent with the rules on switching between data processing services introduced by the **Data Act**. By enabling switching and removing key sources of vendor lock-in, the Data Act seeks to ensure that cloud computing service providers in the EU compete on quality, innovation, and price. It seeks to enable cloud users to freely choose the provider that best meets their needs and combine offers of different providers in a multi-cloud approach.

However, the Data Act does not contain elements to shape up a more competitive offer of European cloud computing services or encourage the entry into the market of a more diverse set of cloud computing service providers.

The Data Act opens the path towards a possible reduction of dependencies on non-EU providers but does not build the road towards a more sovereign and trusted EU cloud computing sector. Its cloud switching and interoperability provisions, however, make it possible for users to embrace European cloud computing services more strongly. The Data Act is thus an enabler for the proposal.

The proposal is also consistent with the **Digital Markets Act (DMA)**. The DMA covers cloud computing services as a core platform service, meaning that cloud computing service providers designated as gatekeepers would have to comply with a set of obligations to increase fairness and market contestability. So far, no cloud computing service provider has been designated as a gatekeeper for their services. However, on 18 November 2025, the Commission opened three market investigations on cloud computing services under the DMA. Two of these market investigations will assess whether two providers should be designated as gatekeepers for their cloud computing services (in other words whether they act as important gateways between business users and end users). The third market investigation

will assess if the DMA can effectively tackle practices that may limit competitiveness and fairness in the cloud computing sector in the EU.

While certain providers of cloud computing services could be regulated under both this proposal and the DMA, the DMA has different objectives and does not contain measures that would actively promote the uptake of sovereign cloud computing services. The DMA only aims at maintaining and promoting a fair and contestable cloud market in the Union, regulating specific behaviours of companies designated as gatekeepers and thus intervenes at a different level than the proposal, which focuses on the uptake and use of the services provided.

The proposal also reinforces key objectives of the **AI Act**. The AI Act harmonises rules for AI systems and general-purpose AI models to be placed on the EU market, improving the functioning of the internal market and promoting the uptake of human-centric and trustworthy AI along the value chain. The AI Act ensures a high level of protection of health, safety and fundamental rights. It does not cover aspects of sovereignty.

The proposal further complements EU's broader digital policy framework, including the **EU Open Source Strategy**, the **Digital Decade Policy Programme** and **Apply AI Strategy.**

The **EU Open Source Strategy** proposes to foster open source for sovereignty, competitiveness and security through a series of focused measures, some of which are proposed in the Cloud and AI Development Act.

The **Digital Decade Policy Programme** focuses on four cardinal points, under which its targets fall, namely (i) a digitally skilled population and highly skilled digital professionals; (ii) secure and sustainable digital infrastructures; (iii) digital transformation of businesses; and (iv) digitalisation of public services. More specifically, the Digital Decade Policy Programme sets out a target for monitoring the deployment of edge nodes, but it does not include either a target for measuring progress in the deployment of compute capacity or data centres in the EU or concrete support measures for their deployment. This proposal complements the Digital Decade Policy Programme by leveraging the existing yearly monitoring exercise, thus creating synergies with the existing framework. It also helps advance all four Digital Decade policy programme cardinal points, notably by establishing concrete measures centred on developing innovative AI-enabling technologies, deploying expanded compute capacity, and creating a trust framework for enhanced use of cloud and AI.

Moreover, the **Apply AI Strategy** sets out concrete actions to harness AI's transformative potential, with a focus on boosting adoption across key industry sectors and the public sector. It also introduces support measures to strengthen the EU's technological sovereignty by tackling cross-cutting challenges in AI development and deployment. The proposal underpins these objectives and contributes to their implementation by introducing targeted measures aimed at supporting the development and deployment of cloud and AI, increasing access to compute capacity and building trust in cloud computing services.

The proposal is fully compatible with the EU's June 2025 **Communication on an International Digital Strategy**. It creates a transparent, non-discriminatory blueprint for digital autonomy that allows the EU to build resilient, sovereign tech infrastructures at home while providing a trusted, legally sound model for international partnerships and multilateral governance abroad. It is fully consistent with the Union's international commitments and partnerships and will secure access to the internal market to entities from partner countries that meet required levels of Union assurance.

- **Consistency with other Union policies**

The proposal complements EU's broader policy framework on cybersecurity and digital resilience.

This proposal needs to be read in conjunction with the proposal for the review of the **Chips Act**, which includes measures to promote investments in advanced semi conductors, increase supply chain resilience and demand creation through increased cooperation between the semiconductor supply chain and end markets.

The **Directive on Security of Network and Information Systems (NIS2)** improves the cybersecurity risk management of cloud computing service providers and data centres in the EU, resulting in greater trust. However, it does not contain measures to boost the uptake and use of such services and is fully focused on technical cybersecurity as opposed to broader sovereignty considerations.

As detailed earlier, the proposal further supplements the **Cybersecurity Act**'s focus on cloud cybersecurity with sovereignty considerations. Certification under the Cybersecurity Act can address technical cybersecurity criteria but is not suited for addressing sovereignty concerns that go beyond these technical elements. Meanwhile, the European Union Agency for Cybersecurity (ENISA) has been working on developing a **European Cybersecurity Certification Scheme for Cloud Services (EUCS)**, which has not yet been adopted. When finalised, it could be leveraged in the framework for sovereign cloud computing services as a way of ensuring that an audited service meets the highest cybersecurity standards. Furthemore, the proposed review of the Cybersecurity Act reinforces the trustworthiness of the hardware and software ICT supply chain.

The proposal also supports the objectives of the **Digital Operational Resilience Act (DORA)**. The Digital Operational Resilience Act shapes compliance obligations for cloud computing service providers. It indirectly covers cloud computing service providers if they provide services to specified financial entities or if their role is significant enough in terms of operational resilience. It has a sectoral scope and is specific to the financial sector. Under the Digital Operational Resilience Act, cloud computing service providers must implement ICT risk management and conduct regular incident response testing to comply with the requirements for critical third-party service providers. The financial institutions concerned, which could be public in nature, must carry out due diligence on the cloud computing service providers they work with.

The proposal also supports the objectives of the **Preparedness Union Strategy**, which identifies dependence on critical digital infrastructure as a systemic risk and calls for a whole-of-government approach to ensuring the continuity of essential services in crisis scenarios. The sovereignty framework established by this Regulation, and in particular the risk assessment mechanism in Article 29, contributes directly to the digital preparedness dimension of that Strategy by ensuring that the cloud and AI services underpinning emergency management, civil protection coordination and disaster response operations are provided at the appropriate Union assurance level. The proposal is therefore consistent with, and supportive of, the Union's broader resilience and preparedness policy objectives.

The proposal is consistent with existing rules on the processing of personal data, including the **General Data Protection Regulation (GDPR)** and the EU-US Data Privacy Framework. However, while the EU-US Data Privacy Framework addresses transatlantic data transfers, it does not remove sovereignty concerns about dependence on third-country providers. The proposal thus complements the EU-US Data Privacy Framework as the notion of sovereignty goes beyond data transfers and relates to operational autonomy too.

The proposal also supplements the **Public Procurement Directives**. Public authorities in the EU rely heavily on non-EU cloud computing service providers and associated problem drivers require a nuanced and targeted sectoral approach, which is not covered by the existing Public Procurement Directives and would be difficult to account for sufficiently through an overarching approach. The proposal therefore provides a sector-specific approach to sovereignty – the many layers of which cannot be addressed in the horizontal acquis that sets out general principles for the design of procurement procedures. The proposal includes complementary award criteria that are also tailored to the specificities of cloud computing services and critical dependencies on third countries in this sector.

The proposal complements the **Digital Networks Act**, which supports the development of a robust, fast, secure, cutting-edge digital networks and thus be beneficial to the deployment of data centres in the EU, for which high-speed, gigabit and beyond connectivity is a prerequisite. The proposal leverages the Digital Networks Act's advancements for connectivity and thus stays focused on the deployment of data centres capacities, not the prior or parallel build-out of the necessary connectivity infrastructure. The Digital Networks Act also addresses the convergence of networks infrastructure, including scenarios where a cloud computing service provider operates an electronic communications network and has so far not been subject to obligations under the **European Electronic Communications Code** although falling into its scope. Thus, the Digital Networks Act will clarify the procedures for connectivity between providers of various networks and other market participants within a broader ecosystem cooperation.

The proposal contributes to the objectives of the **Energy Efficiency Directive** on guiding the data centre industry towards greater energy efficiency. However, beyond transparency and reputational considerations, it does not set incentives for data centre operators to improve their sustainability performance and does not contain measures for accelerating the roll-out of sustainable data centres across the EU or increasing related investment.

Similarly, the **EU Code of Conduct on Data Centre Energy Efficiency** does not concern measures to deploy a data centre, instead focusing fully on practices for operating one. Thus, the proposal provides measures to incentivise the roll-out of energy-efficient data centres, aligning with the **Strategic roadmap for digitalisation and AI in energy**, which seeks to optimise energy consumption in digital technologies while accelerating the EU's twin green and digital transition. To identify which data centres are sustainable, the proposal refers to the rating scheme developed under the Energy Efficiency Directive.

The proposal also complements the **European Grids Package**, which aims to ensure grids are in place and ready to uptake future loads in a horizontal manner. Here, the proposal focuses on data centres as an ultimate client of grid capacity and ensures data centres location considers grid availability, information is exchanged sufficiently in advance to feed into grid planning and hence ensure timely connection of data centres.

The European Grids Package sets out ways in which Member States can accelerate grid connections, including a more efficient structure of their grid connection queue, for example by considering a project's readiness and grid-friendly uses as opposed to a pure first-come-first-served approach. The proposal leverages these considerations.

The proposal also complements the **Renewable Energy Directive** and can leverage it. Data centres may benefit from the increased availability of renewable energy and storage even if they are not themselves covered by the Directive. Proximity to acceleration areas for renewables could also be a relevant factor in designating sites for faster data centre deployment.

The **Industrial Accelerator Act** puts forward measures to accelerate permitting, including setting out the principle of 'one project, one procedure' and establishing a single digital procedure to cover the entire permit-granting process. The Industrial Accelerator Act also requires Member States to designate at least one manufacturing industrial acceleration area or cluster where further business facilitation measures apply, including prioritised access to materials, and access to EU finance. However, as the proposed industrial acceleration measures only account for manufacturing facilities and do not account for the specific needs of data centres as well as their benefits, they have been left out of scope of the Industrial Accelerator Act. Addressing these differences, the proposal complements the general industrial acceleration measures with measures that are tailored to the accelerated deployment of data centres.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for this proposal is **Article 114 of the Treaty on the Functioning of the European Union (TFEU)**, which empowers the EU to adopt measures for improving the functioning of the internal market through the harmonisation of national provisions.

The current fragmentation in data centre deployment is driven by divergent national approaches to capacity expansion, sustainability requirements, and permitting procedures. These risks creating regulatory disparities that could undermine the internal market.

Variations in public procurement practices for cloud computing services, as well as inconsistent sovereignty criteria, may hinder providers' ability to operate seamlessly across Member States, leading to market inefficiencies and unequal competitive conditions.

Given these challenges, EU-level intervention in the form of a legislative proposal is justified under Article 114 TFEU, as it seeks to eliminate barriers to the internal market and levels the playing field for cloud computing service providers.

Additionally, the proposal draws on **Article 173(3) TFEU**, which provides the legal basis for measures aimed at enhancing the EU's industrial competitiveness and innovation capacity. The current shortage of computing capacity in the EU constrains the ability of European industries to fully benefit from the use of cloud and AI technologies, especially those requiring low-latency and high-performance computing. By increasing the availability of energy-efficient compute capacity and the development and deployment of cutting-edge cloud and AI technologies, this initiative directly helps strengthen Europe's industrial competitiveness and technological leadership, in line with the objectives of Article 173(3) TFEU.

Given the proposal's dual objective of remedying internal market distortions and bolstering the EU's industrial competitiveness, it will be adopted as a single legislative instrument under the cumulative legal basis of Articles 114 and 173(3) TFEU. This joint legal foundation provides a unified regulatory response to the interlinked challenges of market fragmentation and strategic industrial capacity-building within the EU's cloud and AI ecosystem.

• Subsidiarity (for non-exclusive competence)

EU action has a clear added value in addressing the problem of limited and geographically concentrated availability of computing capacity. By providing a common approach to accelerating data centre deployment, it enables coherent planning and deployment of computing capacity in a geographically balanced way, while avoiding a race to the bottom and reducing regulatory complexity for investors and data centre operators.

The EU is uniquely positioned to ensure that investment and acceleration policies reflect collective priorities and avoid fragmentation. EU-level action would ensure that all businesses and public administrations can access sufficient compute capacity to meet their needs and is a prerequisite for Europe to become an AI continent.

In addressing the dependence on cloud computing services supplied by non-European providers, EU action delivers benefits that exceed what Member States could achieve individually, especially in addressing the underlying market failures of imperfect information. This will improve the functioning of the internal market and enable cloud computing service providers to grow beyond their national markets.

- **Proportionality**

The proposal adopts a targeted and proportionate approach to address the critical bottlenecks in the single market, specifically the compute capacity deficit and overreliance on third-country providers. The proposed solutions are confined to measures essential for achieving core objectives of the proposal notably the strengthening of the EU technological sovereignty, fostering a competitive EU cloud and AI market, and supporting an enhanced availability of sustainable computing resources in the EU.

By focusing on harmonised standards for sovereign cloud computing services, streamlined data centre deployment, and EU-wide cooperation mechanisms, the proposal avoids excessive regulation while directly tackling the structural barriers that impede the digital advancements across Europe. The chosen measures represent the most suitable and least intrusive means of addressing the identified market and regulatory failures, as they leverage existing EU instruments while introducing only those new provisions necessary for cohesive and efficient implementation.

The proposal will give rise to direct compliance costs, covering both administrative and adjustment expenditures. These are to be borne mainly by national and local public authorities, and businesses such as data centre operators, cloud-computing service providers as well as their subcontractors and private-sector entities operating in sectors listed under Annex I to the NIS2 Directive, so that they comply with the obligations set out in this Regulation.

However, the exploration of different options and their expected costs and benefits has resulted in a balanced design of the instrument. The costs to public authorities will be counterbalanced by the value of reduction of total cost of ownership for IT systems and faster and more reliable procurement processes, while the costs to businesses will be counterbalanced by the value of improved predictability of regulatory direction and reduced fragmentation of national approaches together with administrative simplification.

- **Choice of the instrument**

The Commission proposes a Regulation as the optimal legal instrument for the accomplishment of the proposal's objectives, given its capacity to ensure uniform application and immediate effect across all Member States. A Regulation provides the necessary legal certainty and consistency to fully harmonise the regulatory framework for cloud computing services. This approach is essential to remove single market barriers, particularly in areas such as sovereignty and sustainability standards, where divergent national rules could otherwise undermine the EU's technological sovereignty and competitiveness. Given the geopolitical urgency, including the need to reduce strategic dependencies on third-country providers, a Regulation ensures a rapid, coordinated, and EU-wide response, preventing delays or inconsistencies that could arise from Member States acting greater independence.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

Between October 2024 and November 2025, an extensive stakeholder consultation was carried out comprising the following consultation activities.

Between April and July 2025, the Commission organised a Public Consultation consisting of an online questionnaire and a call for evidence for stakeholders to submit detailed position papers outlining their views and recommendations on the objectives and proposed actions envisaged by the proposal, while also giving direct evidence to inform the design of policy options. A total of 436 responses were received: 243 for the consultation survey and 193 for the call for evidence.

A series of workshops, seminars and roundtables complemented the consultation. These included: (i) the 6th General Assembly and Alliance Forum of the European Alliance for Industrial Data, Edge and Cloud; (ii) roundtables, namely on investment in cloud compute with financial investors, on policy measures to facilitate data centre integration to the EU grid, with European Cloud Service Providers' CEOs on developing sovereign cloud offerings in the EU, and with American Chamber of Commerce; (iii) seminars with industry, academia and public authorities on the economic dynamics of the AI stack; and (iv) presentations on future EU cloud and AI policy with industry.

The Commission also maintained a continuous dialogue with Member States' relevant authorities gathered in the informal Member States Cloud Cooperation Group under the European Alliance for Industrial Data, Edge and Cloud, complemented by targeted bilateral meetings.

In addition, the Commission engaged in further bilateral discussions with third countries, including Japan, Switzerland and the United Kingdom, to present and discuss the considered policy options while gathering insight on best practices and assess the external effect of measures considered.

Finally, the Commission held over 100 bilateral meetings with a diverse array of stakeholders, including industry representatives, academic institutions, think tanks and civil society organisations supported the formulation of the proposed policy options.

- **Collection and use of expertise**

The Commission contracted a consortium led by Technopolis Group to conduct a study to support the evidence collection and analysis stage of the impact assessment preceding the proposal. The study incorporated multiple stakeholder engagement activities, including over 60 targeted interviews, surveys (over 250 replies), and workshops (over 100 participants).

- **Impact assessment**

The proposal is accompanied by a comprehensive impact assessment the final version of which was submitted to the Regulatory Scrutiny Board on 30 April 2026. On 8 May 2026, the Board issued a positive opinion accompanied by a request for further improvements.

- **Fundamental rights**

The proposal has been subject to a comprehensive assessment of its implications for fundamental rights, with particular emphasis on the protection of personal data as guaranteed under Article 8 of the Charter of Fundamental Rights of the European Union. The proposal introduces a framework for sovereign cloud computing services, which establishes stringent

safeguards to ensure that the processing of personal data involving EU citizens complies with EU data protection standards, including the GDPR. By setting these standards, the proposal minimises risks associated with non-compliant data handling while reinforcing trust in digital infrastructure.

One of the core objectives of the proposal is to reduce dependence on third-country providers, whose operations may be subject to non-EU jurisdictions that can permit data access and transfer. Consequently, the proposal enhances the protection of personal data by ensuring that such data remains under the effective supervision of EU authorities, including Member State data protection agencies and the European Data Protection Board. This approach strengthens legal certainty and upholds the right to privacy as enshrined in the Charter.

Furthermore, the proposal fosters a competitive single market for cloud computing services, where providers are fully bound by EU legislation and subject to applicable obligations. This not only improves data availability and continuity but also ensures that EU legal obligations, such as those related to data subject rights and regulatory oversight, are consistently met. By increasing the market presence of EU-based providers, the proposal further embeds fundamental rights protections into the digital ecosystem, offering stronger guarantees against unauthorised access or misuse of personal data. The proportionality of these measures has been carefully considered to balance innovation with the imperative of rights protection, in line with the Charter's principles.

4. BUDGETARY IMPLICATIONS

The budgetary implications of the proposal are described in detail in the accompanying financial statement. In order to effectively implement the initiative, 25 full-time equivalents (FTEs) are required, comprised of 9 establishment plan posts and 16 contract agent posts. This staffing configuration will be achieved through a combination of redeployment and additional recruitment. Specifically, 15 existing staff members will be reassigned from within the Commission to support the initiative, leveraging their expertise and experience in managing similar actions. The necessary staff will be drawn from DG CNECT and DG DIGIT, where they are currently assigned to relevant units or will be redeployed from within the Commission services. To supplement these existing resources, the initiative will require an additional 10 FTEs: of 6 FTEs for DG CNECT and 4 FTEs for DG DIGIT. These additional staff members will be requested to augment the current staffing levels to ensure the initiative's successful implementation and the effective performance of new activities and tasks.

The additional administrative expenditure associated with new tasks described in the proposal will be mostly financed through fee-based revenue streams that fall under internal assigned revenues, thus ensuring a sustainable and viable funding model. Specifically, fee-based streams will be used to support tasks related to joint procurement and to the administration of the EuroCloud initiative intended to make it easier for interested Member States to share idle cloud and data centre capacity.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission should monitor the application of the proposed Regulation and evaluate its effectiveness over time. Five years after its entry into force, the Commission should review the functioning of this proposed Regulation and submit a report to the European Parliament

and to the Council. These reports will be public and detail the effective application and enforcement of the proposed Regulation.

- **Detailed explanation of the specific provisions of the proposed Regulation**

Title I of the proposed Regulation contains the general provisions, including the subject matter (Article 1) and the definitions (Article 2).

Title II contains the provisions that establish the framework for the implementation of development and deployment activities across the cloud and AI ecosystem. The framework is organised into the Cloud and AI Leadership Initiatives and is reinforced by further supporting measures. Under Chapter I, Article 3 sets out general objective of the Cloud and AI Leadership Initiatives aiming to support research and innovation activities and achieve large-scale capacity throughout the Union's cloud and AI ecosystem. Article 4 establishes the operational objectives of the Cloud and AI Leadership Initiatives. Article 5 introduces a network of Experience and Acceleration Centres for AI built on the European Digital Innovation Hubs and aiming to support the achievement of the Cloud and AI Leadership Initiatives objectives. Article 6 sets out the implementation mechanisms for the Cloud and AI Leadership Initiatives. Article 7 requires Member States to adopt a national cloud and AI strategy coherent with the Regulation's objectives within one year of its entry into force. Article 8 establishes criteria for projects to be recognised by the Commission as a frontier AI priority project. Article 9 supports the allocation of AI computing resources tofrontier AI priority projects, while also supporting industrial and physical AI projects and the development and deployment of AI models for the public sector.

Title III sets out the provision on data centre capacity. Under Chapter I, Article 10 sets out the obligations for Member States to designate data centre acceleration zones within their territory, where they are deploying data centre capacity. Article 11 prescribes the conditions within data centre acceleration zones. Article 12 establishes the obligation for Member States to designate single information points, or where possible, upgrade or integrate with the already existing single information points, for data centre operators of data centre projects in data centre acceleration zones and further principles to be satisfied with respect to the responsibilities of the information point. Article 13 addresses the facilitated administrative and permit granting processes for data centre projects deployed in data centre acceleration zones. Under Chapter II, Article 14, lays down the mechanism for expression of interest and conditions and designation by the Commission of data centre strategic projects. Under Chapter III, Article 15 establishes a mechanism for the Commission to monitor the Union progress in increasing the compute capacity available, the volume of demand for data centre capacity, and the size of the capacity gap.

Title IV contains the provision relating to autonomy and adoption. Under Chapter I, Section 1, Article 16 sets out a Union cloud computing sovereignty framework consisting of four assurance levels and introduces the requirements established in Annex II to the Regulation for cloud computing services to be considered as providing Union assurance across level 1 to level 4. Article 17 established a mechanism for cloud computing service providers to be recognised as providing a Union assurance level 1, 2, 3, or 4, where they must submit an application for recognition to the national competent authority of establishment. Article 18 sets out conditions and a mechanism for a possible recognition of third-countries as providing sufficient assurances to allow for cloud computing services controlled from that third country to become eligible to qualify under Union assurance level 3. Section 2, Article 19 sets out the conditions for the conformity self-assessment documenting the alignment against the requirements of the Union assurance level 1. Section 3, Article 20 sets out the framework of

assessment performed by auditing organisations against the requirements of the Union assurance levels 2-4. Article 21 sets out the requirements for audit evidence to be established as part of the third-party assessment of requirements under Union assurance levels 2-4. Article 22 sets out the obligation for the Commission to establish and maintain a central repository of services recognised as offering Union assurance levels 1-4. Article 23 sets out transparency obligations for cloud computing service providers', to report any material changes which may substantiate a resulting change in their recognition as offering Union assurance levels 1-4. Article 24 sets out the penalties and compensation rules applicable to infringement by cloud computing service providers. Section 4, Article 25 sets out the Member States obligations to designate a national competent authority. Article 26 sets out the powers of national competent authorities designated by the Member States. Section 5, Article 27 sets out principles of mutual assistance between Member States national competent authorities in the context of information sharing and investigation for the purpose of this Regulation. Article 28 sets out the principles of cross-border cooperation between Member States national competent authorities in the context of enforcement actions. Under Chapter II, Section 1, Article 29 sets out the obligations for Member States and Union entities to conduct risk assessments to determine the required level of conformity against the Union assurance levels 2-4 for different public sector activities. Article 30 sets out obligations for contracting authorities that procure cloud computing services to procure, as a minimum requirement, Union assurance level 1. Where a risk assessment determines that the activities of such contracting authorities have public order relevance, they must only procure and use services that have been recognised as offering Union assurance levels 2, 3, or 4. Section 2, Article 31 allows for private sector entities within the meaning of the NIS2 Directive to conduct impact assessments with a similar purpose to the ones conducted by Union entities and public sector bodies. Section 3, Article 32 sets out obligations for the Member States contracting authorities to apply Union added value criteria in public procurement of cloud computing services and AI systems within the scope of the Regulation. Article 33 sets out obligations for Member States to monitor their procurement of innovation of cloud computing services and AI systems, introduces a lean reporting framework and creates links to national cloud and AI strategies where Member States must create plans for the achievement of the objectives of this Article. Under Chapter III, Article 34 establishes the European public sector cloud federation ('EuroCloud Federation') and sets out its scope and purpose. Article 35 sets out the conditions applicable to the sharing of data centre services and cloud computing services within the EuroCloud Federation. Article 36 sets out how the Commission can recover the costs incurred in relation to the EuroCloud Federation, including the establishment of the EuroCloud Federation and of the platform facilitating the sharing of services among its members. Chapter IV, Article 37 sets out the conditions for the Commission to carry out procurement activities for Union entities,for contracting authorities from Member States, and for partner organisations selected by the Commission, including by establishing the necessary derogations to the Financial Regulation. Article 38 sets out the necessary arrangements for implementing the common procurement framework, including the governance mechanism. Article 39 sets out the applicable public procurement rules. Article 40 sets out the mechanism for the compensation of costs incurred by the Commission for the operation of the common procurement framework via fees levied on participating contracting authorities. Chapter VI, Article 41 sets out the obligations of the Union entities and public sector bodies to encourager and facilitate thier use of opensource solutions over proprietary ones. Article 42 sets out the requirements on sharing and reuse of software developed by or for Union entities and public sector bodies. Article 43 sets out the obligation for the Commission to provide and maintain an Open Source Solutions Catalogue. Article 44 sets out the rules for the establishment of a network of Member States Open Source Programme Offices.

Title V sets out the final provisions, including the power for the Commission to adopt delegated acts (Article 45) and implementing acts (Article 46), the review clause (Article 47), and the specification of the entry into force and dates of application of the Regulation (Article 48).

2026/0138 (COD)

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)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 and Article 173(3) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Union is committed to become a global leader in artificial intelligence (AI). By enabling faster innovation, greater efficiency and smarter decision-making, AI contributes to substantial economic, environmental and societal gains and is a fundamental driver of competitiveness. In order to fully harness the benefits of AI across the key sectors of the economy, the Union should act with ambition and foresight, advancing its innovation capabilities, strengthening its competitiveness, security of supply, while reinforcing its technological sovereignty and strategic autonomy in cutting-edge digital technologies.

(2) The Union has already laid strong foundations to position Europe as a continent that leads AI development and uptake, in particular through the AI continent action plan communication ([3]) and Apply AI Strategy ([4]). With Regulation (EU) 2023/2854 ([5]) of the European Parliament and of the Council on harmonised rules on fair access to and

---

1 OJ C , , p. .

2 OJ C , , p. .

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'AI Continent Action Plant', 9.4.2025, COM(2025) 165 final.

4 Communication from the Commission to the European Parliament and the Council, 'Apply AI strategy', 8.10.2025, COM(2025) 723 final.

5 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

use of data ('the Data Act') and Data Union Strategy ([6]), the Union has also set up the necessary frameowrk to create a secure and interoperable single market for data, which underpins the development of AI.

(3) The European Parliament, the Council, the Commission and the Member States have committed themselves to cooperate on delivering the Union's technological sovereignty in an open manner, in particular by secure and accessible digital and data infrastructures that enable other technological developsments, supporting the competitiveness and sustainability of the Union's industry and economy, in particular of small and medium-sized enterprises ('SMEs') ([7]) and small mid-caps ('SMCs') ([8]), and the resilience of the Union's value chains, as well as fostering the start-up ecosystem, including through the smooth functioning of the former European digital innovation hubs ('EDIHs'), which have been refocused as the experience and acceleration centres for AI ('Centres for AI').

(4) The Union has become increasingly dependent on a limited number of cloud computing service providers from third countries. Reinforcing the Union's capacity to develop and deploy cloud and AI technologies within its territory has become a strategic priority for the Union's competitiveness, security of supply and technological sovereignty, as highlighted in the report by Mario Draghi on the future of European competitiveness ([9]) and in line with the Strengthening EU economic security Communication ([10]). Those challenges to the Union's cloud and AI ecosystem call for the achievement of large-scale technological capacity building and support related to research and innovation activities and require collective effort by Member States, with the Union supporting the development and deployment of cloud and AI technologies and of large-scale cloud computing capacity.

(5) Those dependencies translate not only into limited market shares for the European cloud computing service providers, but also into significant risks for the Union's operational autonomy, resilience and security. The Council has called for a Cloud and AI Development Act to include common criteria for sovereign cloud computing services, allowing market transparency risks and risks associated with dependencies, including extraterritorial effects of legislation adopted by third countries, to be addressed ([11]).

(6) A framework for increasing the Union's resilience and security in the field of cloud and AI technologies should be established, reinforcing the Union's cloud and AI ecosystem by reducing dependencies, enhancing technological sovereignty, stimulating investment and strengthening the capabilities, security, adaptability and resilience of the Union's cloud and AI supply chain.

---

6 Communication from the Commission to the European Parliament and the Council, 'Data Union Strategy', 19.11.2025, COM(2025) 835 final.

7 As defined in Title I, Article 2, of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

8 As defined in point 2 of the Annex to Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

9 *The future of European competitiveness. Part A, A competitiveness strategy for Europe* ('the Draghi report'), September 2024, https://data.europa.eu/doi/10.2872/9356120.

10 Joint Communication from the Commission to the European Parliament and the Council, 'Strengthening EU economic security', JOIN(2025) 977 final.

11 Council Conclusions on European Competitiveness in the Digital Decade, 5.12.2025, https://data.consilium.europa.eu/doc/document/ST-16430-2025-INIT/en/pdf.

(7) The framework pursues separate objectives, relying on two distinct legal bases.

(8) First, it is necessary to strengthen the competitiveness, capacity and resilience of the cloud and AI technological and industrial base of the Union in accordance with Article 173(3) of the Treaty on the Functioning of the European Union (TFEU). Such measures should not entail the harmonisation of national laws or regulations. To that end, this Regulation establishes the Cloud Leadership Initiative and the AI Leadership Initiative (the 'Cloud and AI Leadership Initiatives') to foster the development of cutting-edge cloud and AI technologies and facilities and ensure their widespread deployment, bridging the gap between the Union's advanced research and innovation capabilities and their sustainable exploitation.

(9) Second, the available compute capacity and resilience of the cloud and AI ecosystem can best be addressed through Union harmonisation measures on the basis of Article 114 TFEU. A single coherent regulatory framework harmonising certain conditions for service providers and deployers of cloud computing services, including capacity building and provision of cloud computing services, is necessary to ensure the functioning of the internal market.

(10) The definition of 'cloud computing service' in this Regulation should be the same as that in Article 6, point (30), of Directive (EU) 2022/2555 of the European Parliament and of the Council ([12]), which defines a 'cloud computing service' as a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. This definition of 'cloud computing service' encompasses on-demand access to AI systems as defined in Article 3, point (1), of Regulation (EU) 2024/1689 ('Artificial Intelligence Act') ([13]) of the European Parliament and of the Council, hosted and operated remotely. Only the delivery and making available of an AI system forms part of the service. The AI system itself and its underlying model are excluded from the scope of this definition.

(11) The Cloud and AI Leadership Initiatives should reinforce the competitiveness and resilience of the cloud and AI technological and industrial base of the Union, while strengthening the innovation capacity of its cloud and AI ecosystem and achieving the deployment of large-scale digital infrastructures, in line with the objectives set out in the AI continent action plan and the Apply AI Strategy. In particular, the Cloud and AI Leadership Initiatives should increase the cloud and data centre capacity of the Union, while advancing cutting-edge cloud and AI technologies together with broad cloud and AI adoption across the Union's economy. It should also bring advanced research in sector-specific deployment of frontier, physical and industrial AI. The Apply AI Strategy should extend the ambitions and objectives set out in the AI continent action plan and should be updated where necessary to take account of the latest technological developments and progress made in the Cloud and AI Leadership Initiatives.

---

12 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

13 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

(12) In order to pursue the achievement of those general objectives, the Cloud and AI Leadership Initiatives should support complementary operational objectives designed as actionable initiatives to be implemented at Union level.

(13) To enable data centres to act as key enablers of a sustainable digital transition, the Cloud and AI Leadership Initiatives should support research and innovation capacities for the development of data centre technologies incorporating principles of energy and resource efficiency by design and throughout operations, with a view to achieving large-scale sustainability. This includes advancing resource and utilisation-efficient computing technologies, such as the optimisation of energy and water efficiency, the use of emerging quantum computing technologies, the development of AI-powered technologies for server efficiency, the integration of computing infrastructure with energy grids, the promotion of clean energy adoption and on-site energy generation in data centres. The Cloud and AI Leadership Initiatives should also provide access to pilot lines for data centre technologies to steer and accelerate innovation uptake in the market. Such pilots should function as demonstration facilities for cutting-edge data centre and edge semiconductor technologies, quantum computing prototypes and AI-powered data centre operation tools.

(14) The Cloud and AI Leadership Initiatives should also support research, development activities and the uptake of cloud stack technologies with a view to closing the capacity gap and strengthening the technological autonomy of the Union. In particular, the Cloud and AI Leadership Initiatives should foster the development of cloud computing stacks alternatives for strategic sectors. It should also facilitate the development of AI-optimised servers and software including processors and accelerators manufactured and designed in the Union, such as those developed under Regulation (EU) 2026/XXX ([14]) of the European Parliament and of the Council. In addition, both the Cloud and AI Leadership Initiatives under this Regulation and the Chips for Europe Initiative 2.0 supported by that Regulation should foster the co-design and cross-optimisation of hardware and software development and the integration of AI computing infrastructures. Furthermore, the Cloud and AI Leadership Initiatives should support the complementary development and deployment of a smart and secure middleware cloud platform for common European data spaces, in accordance with the Data Union Strategy.

(15) The Cloud and AI Leadership Initiatives should also promote the development of technologies relying on open standards, open specifications and open source and foster the development of innovative, competitive and resilient cloud and AI technologies. It should foster the work on open standards and specifications and the creation of open-source software foundations supporting the design, development and maintenance of open-source components, in particular by providing governance and coordination mechanisms and facilitating the pooling of resources. The Cloud and AI Leadership Initiatives should also create a catalogue of software tools including open source in order to enable federation with existing catalogues for the private and public sectors and to develop a one-stop-shop for open-source resources in the Union.

(16) Frontier AI technologies are advancing rapidly and are expected to have a profound impact on the Union's economy and society. As those technologies have become critical strategic assets, strengthening the Union's capacity to develop and govern them is essential to ensure that the AI transition is aligned with Union values, safety

[14] References to Chips Act 2.0 to be added once adopted. See Commission proposal [add reference once published]

standards and long-term economic interests. By supporting pioneering projects, the Union should scale up essential breakthroughs to maintain a competitive edge in the global digital economy. Fostering the development of frontier AI technologies as strategic assets should also reduce current dependencies on third-country technologies and strengthen the Union's AI ecosystem.

(17) The emergence of physical AI, which refers to AI systems and models capable of perceiving the physical environment and executing complex actions within that environment, represents a promising frontier where advanced digital intelligence is integrated into tangible systems, such as robotics, autonomous drones and self-driving vehicles. Physical AI is essential to mitigate external dependencies and foster industrial competitiveness and strategic autonomy. It requires a dedicated approach to data and computing infrastructure. It is therefore necessary to facilitate the collection and preparation of high-quality data and access to computing resources. Furthermore, targeted support for the testing and validation of physical AI models and systems in diverse real-world environments is necessary to ensure their robustness and reliability.

(18) The digital transformation of the Union's key industries is a central pillar of the apply AI strategy. Accelerating the uptake of AI across those strategic sectors is essential to maintaining global competitiveness and increasing societal benefits. The Cloud and AI Leadership Initiatives should accelerate the development and uptake of industrial AI across the Union's strategic industrial and service sectors, while fostering the technological development of highly capable sector-specific AI models designed to meet the operational requirements of the industries prioritised under the Apply AI Strategy, such as healthcare, transport, including aerospace, automotive, manufacturing, defence and space, climate and environment and agri-food. The Cloud and AI Leadership Initiatives should also accelerate the development of service sectors prioritised in the Apply AI Strategy and scientific discovery as priorities in the European strategy for AI in science, in line with COM(2025) 724 final.

(19) In healthcare, those advancements should improve the accuracy of clinical decisions and transform the pharmaceutical sector. In the automotive sector, they should support the development, testing and deployment of innovative software platforms contributing to the Union industrial leadership in software defined vehicles and autonomous driving. The Cloud and AI Leadership Initiatives should also reduce obstacles to test and deploy AI models, in particular within cities and regions contributing to the development of Union leadership in software defined vehicles and autonomous driving. Furthermore, Member States should facilitate the development, testing and deployment of AI systems for autonomous driving, including through cooperation with the Centres for AI, the automotive industry, suppliers, cities and regions, with a view to enabling the safe and trustworthy deployment of AI-enabled connected and autonomous mobility solutions across diverse European environments. In manufacturing, the Commission should facilitate data pooling across industrial sectors through trusted third parties to train specialised AI models, ensuring a sufficient volume of training data, while strictly preserving intellectual property rights. Secure and verifiable compute approaches should be explored to enable the use of AI in sensitive contexts. In the defence sector, where AI has emerged as a disruptive technology with significant impact on security and defence, the Cloud and AI Leadership Initiatives could support the development of advanced capabilities in full complementarity with, and without prejudice to, dedicated Union instruments in support of the defence industry, including the European defence fund ('EDF') and the European defence industry programme ('EDIP'). In the space sector, digital advances

should transform the way space assets, services and data flows are operated and used, and in the field of transport, digital advancements in aviation should transform the way operations are managed, with AI harnessing decades of available mission, operational and observation data. In the field of climate and environment, geospatial AI should be developed, in particular by leveraging Earth observation data from the Copernicus programme and the capabilities of the Union Space and connectivity programmes in general ([15]). In agriculture, AI can turn data from sensors, satellites and farm machinery into actionable insights for farmers. It can strengthen competitiveness and resilience, for instance by improving yield forecasting, enabling early pest and disease detection, optimising irrigation and fertiliser use, and supporting more sustainable food production. As the deployment of AI in industrial contexts requires rigorous validation in real-world environments, the Union should provide industrial actors with cloud-based AI tools and testing environments.

(20) The Union should also foster the availability of highly secured computing infrastructures for the training, testing and deployment of defence-related AI models and systems.

(21) As AI agents have become increasingly capable and AI applications have become more deeply embedded in real-world business scenarios, industry is rapidly evolving towards a new paradigm that equips such systems with autonomous execution capabilities. This transition to a new paradigm requires a robust technical framework to ensure the safety, accuracy and legal compliance of those systems, given the stringent engineering requirements pertaining on AI platforms. Accordingly, the Cloud and AI Leadership Initiatives should aim to establish sovereign and secure AI platforms dedicated to the large-scale deployment and orchestration of advanced AI agents. Those platforms should be supported by innovative orchestration frameworks that ensure transparency and accountability in multi-agent interactions. It is also necessary to facilitate the development of rigorous testing and experimentation methodologies of AI agents and orchestration to minimise unintended autonomous behaviour.

(22) The Cloud and AI Leadership Initiatives should increase the development and adoption of AI models and systems across the Union's public sector. In particular, AI models and systems should be used to support better decision-making, simplify administrative procedures and reduce unnecessary burdens, in particular for critical public domains such as healthcare where data reuse for AI models and tools should be facilitated while ensuring security and data protection. To that end, it is appropriate to take measures to enhance the quality of public sector data and promote the sharing and reuse of training data and AI models across the Union public sector, thereby avoiding fragmentation and enabling the scaling-up of successful, user-oriented solutions.

(23) The Cloud and AI Leadership Initiative should help accelerate the adoption of AI and cloud computing on a large scale, including at regional and local level. Broad adoption of AI in private and public sectors should be promoted through the network of Centres for AI. Harnessing this network, complementary support measures should be developed, to help achieve the target of digital transformation of businesses set in

[15] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69, ELI: http://data.europa.eu/eli/reg/2021/696/oj).

Decision (EU) 2022/2481 of the European Parliament and of the Council ([16]) ('the Digital Decade Policy Programme 2030'). Furthermore, a dedicated curriculum on cloud computing and AI skills should be developed to equip workers in both the public and private sectors with advanced competencies to reduce dependence on non-EU providers and develop next-generation capabilities, in line with the Union policies in the field of education, training and skills including the Union of Skills communication ([17]).Where relevant, the curriculum should be built on relevant European initiatives, including the AI Skills Academy, the Centres for AI and the Interoperable Europe Academy, and include the participation of stakeholders with the necessary expertise.

(24) The Cloud and AI Leadership Initiatives should also ensure the uptake of cloud computing services provided by European cloud computing service providers across the public and private sectors to ensure that cloud adoption is consistent with the objective of strengthening the Union's technological autonomy, particularly in sectors such as healthcare and education which involve the processing of critical data. This objective could leverage the outcomes of relevant European digital infrastructure consortiums ('EDICs'), including shared infrastructure, common standards and best practices. The Cloud and AI Leadership Initiatives should support the establishment of the European public-sector cloud federation ('the EuroCloud Federation') under this Regulation to facilitate the sharing of secure and resilient public-sector data centre services and cloud computing services. Moreover, the Cloud and AI Leadership Initiatives should support procurement activities carried out by the Commission for Union institutions, agencies and bodies ('Union entities'), but also national contracting authorities across the Union, as the procurement of digital services should not only advance the digitalisation of public-sector bodies, but also enable them to utilise their purchasing power and accelerate the adoption of resilient and secure digital solutions.

(25) Member States should establish Experience and acceleration centres for AI ('Centres for AI') with a view to ensuring an appropriate coverage of their territory. Centres for AI need to act as regional and local accelerators for the uptake and deployment of AI, cloud computing and other advanced technologies across the Union, supporting SMEs, SMCs and public sector bodies in their digital transformation. In order to facilitate the integration of AI into strategic industrial sectors, Centres for AI should also establish synergies with initiatives launched under the Data Union Strategy. By providing expertise, testing, skills and innovation support, Centres for AI should reinforce the competitiveness and resilience of the Union's AI industrial base while strengthening the innovation capacity and widespread deployment of AI and other advanced technologies across the Union. The network should build on the network of European digital innovation hubs. The network will collaborate closely with other initiatives supporting the uptake of AI and other advanced technologies such as testing and experimentation facilities and AI factories. It will be built on skills-related initiatives, including the Digital large scale skills partnership under the Pact for skills and the skills academies, including the AI Skills Academy.

(26) The implementation of the Cloud and AI Leadership Initiatives should be entrusted to the Commission and Member States. The implementation of the Cloud and AI

---

16 Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, (OJ L 323, 19.12.2022, p. 4, ELI: http://data.europa.eu/eli/dec/2022/2481/oj).

17 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'The Union of Skills', 5.3.2025, COM(2025) 90 final.

Leadership Initiatives should, where relevant, also be entrusted to any other structure with the appropriate expertise and resources. In particular, without prejudice to the next (2028-2034) multiannual financial framework, it should be possible to entrust the implementation of the Cloud and AI Leadership Initiatives to joint undertakings, such as the Smart Networks and Services Joint Undertaking ('the JU') established by Council Regulation (EU) 2021/2085 ([18]) or the European High Performance Computing Joint Undertaking ('the EuroHPC JU') established by Council Regulation (EU) 2021/1173 ([19]) and, where relevant, their successor.

(27) The Cloud and AI Leadership Initiatives' operational objectives should, in particular, be implemented by setting ambitious, forward-looking objectives that aim to go beyond the current state of the art in infrastructure development, cloud computing and AI. The Cloud and AI Leadership Initiatives should therefore support major strategic 'grand challenges' focusing on the development and deployment of cutting-edge cloud and AI technologies and infrastructure of key importance for the Union. Those grand challenges should build on those established in Regulation (EU) 2026/XXX [Chips Act 2.0] on a framework of measures for strengthening Europe's semiconductor ecosystem, aimed at enabling semiconductor technologies underpinning AI, cloud computing, data centres and edge infrastructures.

(28) The Cloud and AI Leadership Initiatives may be supported by funding from Union programmes and other instruments, in particular from Horizon Europe and the digital Europe programme, as well as the InvestEU programme, in accordance with Regulation (EU) 2021/694 ([20]), Regulation (EU) 2021/695 ([21]) and Regulation (EU) 2021/523 ([22]).Under the 2028-2034 multiannual financial framework, the Cloud and AI Leadership Initiatives could continue receiving support under successive Union programmes, subject to their adoption and in accordance with their respective legal bases.

(29) In addition to receiving funding under Union programmes, the Cloud and AI Leadership Initiatives may be supported by Member States through research, development an innovation measures, in line with the applicable State aid rules, ensuring that national policies and Union policy are mutually consistent, as well as through private-sector investments. In particular, private-sector stakeholders should be encouraged to take into consideration the Cloud and AI Leadership Initiatives when developing their investment strategies for cloud computing and AI. In so doing, private investments can help provide a coherent and coordinated investment pathway

---

18 Council Regulation (EU) 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014 (OJ L 427, 30.11.2021, p. 17, ELI: http://data.europa.eu/eli/reg/2021/2085/oj).

19 Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. 3, ELI: http://data.europa.eu/eli/reg/2021/1173/oj).

20 Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/694/oj).

21 Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/695/oj).

22 Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme and amending Regulation (EU) 2015/1017 (OJ L 107, 26.3.2021, p. 30, ELI: http://data.europa.eu/eli/reg/2021/523/oj).

aligned with the broader policy objectives and long-term implementation goals set out by the Cloud and AI Leadership Initiatives.

(30) The Commission should receive advice from stakeholders with appropriate expertise on the implementation of the Cloud and AI Leadership Initiatives. The Commission should, in particular, foster cooperation with existing expert and advisory forums, such as the Alliance for Industrial Data, Edge and Cloud, the Apply AI Alliance and the Industrial Alliance for Semiconductors. The Alliance for Industrial Data, Edge and Cloud should act as an exchange forum for various stakeholders in next-generation edge and cloud technologies, including businesses, Member States' representatives and other relevant experts. It should help the Commission to design strategic investment road maps to enable the next generation of highly secure, distributed, interoperable and resource-efficient computing technologies. The Apply AI Alliance should act as a coordination forum for AI stakeholders and policymakers to advance the discussion on the potential of AI in strategic Union sectors. The Apply AI Alliance should continue to help implement the objectives of the Apply AI Strategy, in particular by organising industrial workshops, identify and assess new AI use cases in strategic sectors and call for specific supporting policy actions. Alongside the Apply AI Alliance, the AI Observatory should provide robust indicators to assess the impact of AI in strategic sectors, monitor technological developments and trends, as well as the changes it may bring to the labour market.

(31) The Cloud and AI Leadership Initiatives should enhance synergies with actions currently supported by the Union and Member States, including under Horizon Europe and the Digital Europe programme, as well as Council Regulation (EU) 2021/1173 and Regulation (EU) 2026/XXX [Chips Act 2.0] on a framework of measures for strengthening Europe's semiconductor ecosystem. The Commission and the Member States should ensure consistency, complementarity and synergies between the Cloud and AI Leadership Initiatives, and relevant national and regional strategies, programmes and investment plans, including those implemented under national reform programmes, smart specialisation strategies, recovery and resilience plans and other national or regional funding instruments supporting the objectives of the Cloud and AI Leadership Initiatives. Such coordination should aim to maximise the impact of public investments, avoid duplication of funding, promote alignment of priorities across governance levels, and facilitate the scaling-up and deployment of results across the Union.

(32) In order to ensure that the policies of the Union and the Member States are mutually consistent, Member States should adopt national strategies to help achieve the Union's objectives on the development of cloud and AI, in line with the AI continent action plan and the Apply AI Strategy. The national strategies should notably include the 'AI first' principle defined in the Apply AI Strategy, urging organisations to reflect on their business processes, considering the needs of an opportunities offered by AI, while taking into consideration the potential risks. The national cloud and AI strategies should also be aligned with the associated digital targets set under Decision (EU) 2022/2481 ([23]), in particular on the adoption of cloud computing services, big data and AI by at least 75% of Union enterprises for their business operations, and the deployment of at least 10 000 climate-neutral highly secure edge nodes in the Union,

[23] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ L 323, 19.12.2022, p. 4, ELI http://data.europa.eu/eli/dec/2022/2481/oj).

while ensuring low latency. The measures adopted under the national strategies could inform the national digital decade strategic road maps (the 'national road maps').

(33) Where a Member State has already adopted a national strategy that adequately covers the objectives set out in this Regulation, it should not be required to adopt another strategy. However, if a Member State identifies gaps in its existing strategy in light of those objectives, it should update it accordingly. The European Artificial Intelligence Board established by the Artificial Intelligence Act ('the AI Board') plays a central role in ensuring the consistent and effective implementation of Union AI policy. As cloud computing underpins and enables AI, the AI Board should serve as a platform to facilitate cooperation and coordination of AI adoption-related activities between the Union and the Member States. In order to perform this task, the AI Board should have the necessary expertise and appropriate participation.

(34) Given the unprecedented scale of resources required for frontier AI development, it is necessary to set criteria for the designation of a project as a frontier AI priority project. Such projects should support the development and scaling-up of frontier AI technologies, notably in the sector of cybersecurity. In view of their technical complexity and capital-intensive nature, the projects require a collaborative approach at Union level. It is therefore appropriate to require them to involve broad participation from entities across the Union, in particular through EDICs established pursuant Decision (EU) 2022/2481 or any other legal structure capable of representing a meaningful share of the Union's interest.

(35) The allocation of sufficient AI computing resources to frontier AI priority projects should be of strategic importance to the Union and the Member States. The Union should match, on a proportional basis and within the limits of available European high-performance computing ('EuroHPC') capacity, the AI computing resources contributed or committed by the Member States to the designated frontier AI priority projects. The Union and the Member States should also provide sufficient compute time for AI industrial innovation, physical AI and public sector AI projects. This is without prejudice to the rules and procedures laid down in Council Regulation (EU) 2021/1173. The EuroHPC JU access policy should be accommodated to reflect the allocation of such computing resources in an efficient, transparent and timely manner without prejudice to the continuity of ongoing operations and the rights of projects already benefiting from allocated EuroHPC AI computing resources.

(36) To achieve the Union's AI ambitions, it is necessary to strengthen and invest in digital infrastructures, including cloud and edge capacity enabling training, fine-tuning, deployment and real-time operation. The deployment of data centres across the Union is lagging and remains concentrated in a limited number of established hubs, creating structural imbalances between Member States and inefficiencies such as higher costs, increased latency for peripheral regions, unequal opportunities for businesses and slower digital transformation. Increasing and geographically balancing data centre capacities across the Union is also key to reducing dependencies on external infrastructures, thus mitigating economic security risks and supporting the competitiveness, resilience and sovereignty of the Union.

(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 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.

(38) Where capacity is being deployed on the territory of Member States, acceleration zones should be designated where the development, expansion and modernisation of data centres may be facilitated . The designation of such zones should help address the Union capacity gap and increase the Union's competitiveness, autonomy and technological resilience, while ensuring compliance with applicable Union law, including requirements relating to energy efficiency and environmental protection. Sufficient and timely energy supply to the acceleration zones constitutes a fundamental enabling condition for their effective deployment and for the development of data centre capacity across the Union. Reliable and accurate information on future energy demand contributes to cost-effective grid development. Member States should therefore prepare an analysis for each acceleration zone, identifying its current and future energy needs. Such analysis should serve the purpose of providing information for the national grid planning thereby contributing to purposeful anticipatory grid investments and faster energy connections for the acceleration zone. When defining the scope, Member States should take into account the availability of relevant transport and network infrastructure. The results of these assessments should be reflected in national network development plans to adequately capture future points of energy demand in upcoming grid planning. To ensure that acceleration zones enable the right conditions for the deployment of capacity, Member States should facilitate clear and efficient procedures for grid connection and flexible connection agreements and should clarify the conditions for grid connection pursuant to Directive (EU) 2019/944 to data centre operators. An upcoming legal proposal to future-proof electricity bills in the EU will provide incentives to make an optimal and cost-effective use of the grid infrastructure and incentivise system-friendly consumption. Power purchasing agreements ('PPAs') are important instruments for data centres as they provide long-term price stability, while enabling data centre operators to procure clean electricity at scale, thereby supporting reliable operations and the transition to a clean energy system. Member States should therefore promote the uptake of PPAs, also in acceleration zones, by removing unjustified barriers and disproportionate or discriminatory procedures or charges, with a view to providing price predictability.

(39) When setting sustainability requirements for data centres deployed in data centre acceleration zones, Member States should ensure that the key performance indicators as defined in Commission Delegated Regulation (EU) 2024/1364 ([24]) in accordance with Directive (EU) 2023/1791 of the European Parliament and of the Council ([25]) are used. The objective is to ensure consistent environmental standards, increase energy efficiency and support the Union's broader climate, environmental and sustainability goals in acceleration zones. Furthermore, to prevent speculative reservation of

[24] Commission Delegated Regulation (EU) 2024/1364 of 14 March 2024 on the first phase of the establishment of a common Union rating scheme for data centres (OJ L 2024/1364, 17.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1364/oj).

[25] Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast) (OJ L 231, 20.9.2023, p. 1, ELI: http://data.europa.eu/eli/dir/2023/1791/oj).

resources in acceleration zones, ensuring fair, reasonable and non-discriminatory access that preserves effective competition and supports the timely and efficient development of acceleration zones, Member States should ensure that the allocation and use of resources within those zones takes place on fair, reasonable and non-discriminatory terms and does not give rise to any speculative reservation or foreclosure practices capable of impeding effective competition or the effective development or use of those zones.

(40) To facilitate and accelerate the deployment of data centre projects in acceleration zones, Member States should designate single information points or where possible, upgrade or integrate with those designated pursuant to Regulation (EU) 2024/1309 of the European Parliament and of the Council ([26]).

(41) Regulation (EU) 202X/XXX [on speeding-up environmental assessments] ([27]) establishes a common acceleration framework for environmental assessments to boost the Union's roll-out of key technologies, reduce dependencies and increase competitiveness. Procedures linked to environmental assessments should be accelerated and streamlined for plans, programmes and projects across all sectors of the economy while maintaining high levels of protection of human health and the environment. Some sectors may, however, require faster environmental assessments. To ensure the coherence of the legal framework for environmental assessments, while accommodating the need for accelerated deployment in certain strategic sectors, Regulation (EU) 202X/XXX [on speeding-up environmental assessments] establishes a dedicated toolbox. Given their role in ensuring the achievement of the Union's climate and environmental objectives through their contribution to improving energy efficiency, enabling clean energy integration, and providing the infrastructure needed for smarter grids, transport systems, and low-carbon technologies, and their contribution to the Union's resilience and economic security by ensuring reliable infrastructure in the Union to protect critical services and strengthening the Union's capacity to operate independently, data centre projects deployed in acceleration zones should be considered strategic projects within the meaning of Regulation (EU) 202X/XXX [on speeding-up environmental assessments] and therefore benefit from the dedicated toolbox established under that Regulation. Member States should establish an aggregated baseline permit reflecting the specific characteristics of each identified acceleration zone. That aggregated baseline permit issued by public authorities should cover the permits commonly required for such activities within the area, excluding the grid connection permits.

(42) It should be possible for the Commission to designate as strategic projects data centre projects that significantly contribute to the Union's digital and energy sectors and that meet clear criteria. Considering the importance of the data centre strategic projects, Member States may, without prejudice to Articles 107 and 108 TFEU, apply support measures in a proportionate manner to those projects. When planning such support measures, Member States should, where applicable, make use of the relevant frameworks for providing public support. Strategic projects should address a market

---

[26] Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act) (OJ L 2024/1309, 8.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1309/oj).

[27] Add reference to the Regulation on speeding-up environmental assessments once adopted. See Commission proposal COM(2025) 984 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0984.

failure in a proportionate manner, without duplicating or crowding out private financing, while ensuring clear Union added value.

(43) Data centre strategic projects should be granted support from Union programmes, funds and financial instruments, in accordance with the objectives set out in the regulation establishing those funds and programmes and without prejudice to the next (2028-2034) multiannual financial framework. In particular, those strategic projects should be granted the competitiveness seal where they fulfil the conditions set out in Regulation (EU) 2026/XXX [on establishing the European Competitiveness Fund] (ECF') ([28]), as high-quality projects that contribute to the objective of the European Competitiveness Fund.

(44) To foster the strategic deployment of data centre capacity across the Union, the Commission should monitor the available compute capacity and the volume of demand for data centre capacity and identify the size of the capacity gap across the Union. Such monitoring may be used by the Commission to inform its possible recommendations. To guide Member States in accelerating the deployment of data centre capacity, the Commission may recommend, where appropriate, measures to address the identified Union capacity gap. In accordance with the Digital Decade Policy Programme 2030, the Commission should also review the digital decade targets to reflect the technical, economic or societal developments and the evolution of the Union's priorities in that regard.

(45) This Regulation should apply to Union institutions, bodies, offices and agencies ('Union entities') when carrying out procedures for the procurement of cloud computing services and AI systems falling within the scope of this Regulation.

(46) The Union still remains critically dependent on a limited number of cloud computing service providers subject to the control of third countries or legal entities established in third-countries. This exposes the Union to critical strategic dependencies and concentration risks, including vulnerabilities arising from the extraterritorial application of third-country laws, potential disruptions affecting the continuity, quality and resilience of cloud computing services, reduced control and oversight over personal and non-personal data and infrastructure, and the risk of undue economic or political influence being exercised through the control by third countries or legal entities established int third-countries of cloud computing services. Against this background, the ability of the Union and its Member States to retain control over infrastructure, data, assets and technology systems under Union and national jurisdiction has become an imperative policy objective.

(47) Existing Union law addresses cybersecurity, data protection, interoperability and data portability requirements which cloud computing services are subject to. However, there is no cross-cutting Union regulatory framework establishing a harmonised understanding of what constitutes a trusted cloud computing service for mitigating such risks. Some Member States have developed or are in the process of developing national approaches to identifying national sovereign services. However, national measures do not adequately address the cross-border issues related to the Union's lack of sovereignty in the cloud computing ecosystem and risk fragmenting the Union internal market and undermining common goals of autonomy and sovereignty.

---

[28] Add reference to Regulation on establishing the European Competitiveness Fund once adopted. See Commission proposal, COM(2025) 555 final/2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0555R%2801%29.

(48) Cloud computing service providers have launched tailored versions of their service offerings in response to the Union's growing concerns over sovereignty. However, those versions do not address the core sovereignty issues allowing for the extraterritorial reach of third-country laws and the possible degradation or disruption of the service. Consequently, the Union will not ensure autonomy or control over its data, assets and digital infrastructure. The current framework therefore needs to be complemented by targeted actions at Union level by introducing a harmonised mechanism that can strengthen the Union's long-term strategy for technological autonomy, control and resilience in the cloud and AI ecosystem.

(49) Against this background, the significant increase in public order concerns – including, for example, economic security risks – requires effective and coherent implementation of safeguards for activities supported by the Union budget. In the context of Union entities, Article 136 of Regulation (EU, Euratom) 2024/2509 ([29]), sets out the scope, rules and procedures for identifying and implementing sensitive public procurement procedures.

(50) To protect public order, it is therefore necessary to specify the conditions that Union and Member States' contracting authorities should use in public procurement procedures of cloud computing services. The consideration of possible exposure to risk is fundamental when selecting appropriate mitigation measures to preserve the public order of the Union and Member States. The Union and Member States being critically dependent on a limited number of cloud computing service providers subject to the control of a third country or a legal entity established in a third-country may lead to risks such as misuse (i.e. manipulation, remote access and control, sabotage, weaponisation), access to information (i.e. access to sensitive information, unauthorised communication, technology leakage, data manipulation or exfiltration, espionage) and dependency vulnerabilities (i.e. political and/or economic coercion, for example by using vendor or technology lock-ins, embargos or sanctions, monopoly pricing damaging the financial interest of the Union and Member States).

(51) To address those risks and provide for the appropriate mitigation measures, it is necessary to establish a Union cloud computing sovereignty framework determining criteria for trusted cloud computing services. To cater for the nuanced and layered nature of sovereignty, the framework should provide for four different levels of trusted offers ('Union assurance levels').

(52) The Union assurance levels should provide for a proportionate framework to ensure that public order is preserved by maintaining control and agency by public-sector bodies. Most public services would not require the highest levels of assurance. In some specific cases Union assurance levels 3 or 4 may be considered necessary and proportionate in preserving public order. The risk assessment to be performed by Member States and Union entities ensures that the principles of proportionality and subsidiarity are complied with, by assessing the specific cases in which protection of public order requires the highest level of assurance.

(53) It is important that national competent authorities of establishment of the cloud computing service provider can assess whether cloud computing service providers aiming to provide their cloud computing services to Union entities and public sector bodies offer the appropriate assurance level. A mechanism for recognition of cloud

[29] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) (OJ L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

computing services that either have an EU statement of conformity against Union assurance level 1 or have received a 'positive' audit opinion and audit report by an auditing organisation has been established. Once the mechanism of recognition has been positively concluded, the cloud computing service is recognised across the Union as offering the appropriate Union assurance level. In the interest of clarity, simplicity and effectiveness, the powers to supervise and enforce the obligations relating to the cloud computing sovereignty framework should be conferred to the competent authorities in the Member State where the main establishment of the cloud computing service provider is located.

(54) In order to demonstrate compliance with Union assurance level 1, cloud computing service providers should have sole responsibility for carrying out conformity self-assessments by applying the relevant criteria for that Union assurance level. Such self-assessments should be based on documented evidence, internal control procedures and continuous monitoring that are sufficient to demonstrate that the applicable criteria have been fulfilled.

(55) Independent audits are an important tool for monitoring the compliance of cloud compuring services provided by cloud computing service. 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.

(56) The audit report should be substantiated to give a meaningful account of the activities undertaken and the conclusions reached during the audit. It should help provide information for, and where appropriate suggest improvements to, the measures taken by the cloud computing service providers to comply with the applicable criteria and their obligations under this Regulation. The audit report should include an audit opinion based on the conclusions drawn from the audit evidence obtained. A 'positive opinion' should be given where all evidence shows that the provider complies with the audit criteria and obligations set out by this Regulation. A 'negative opinion' should

be given where the auditing organisations considers that the provider does not comply with the criteria set out in this Regulation. Where the audit opinion cannot reach a conclusion on specific aspects that fall within the scope of the audit, an explanation of the reasons why this was not possible should be included in the audit opinion. Where applicable, the report should include a description of specific points that could not be audited, and an explanation as to why they could not.

(57) The establishment of a central repository of recognised Union-assured cloud computing services is necessary to facilitate the secure and efficient storage, access and exchange of relevant information between public sector customers of services offering Union assurance levels, auditing organisations, competent authorities and the Commission.

(58) To ensure the continued accuracy and reliability of the status of cloud computing services as offering Union assurance levels pursuant to the cloud sovereignty framework, providers should be required to promptly report any relevant information or material changes in circumstances to the auditing organisation and the competent authorities of establishment. That information should enable the auditing organisation to reassess, amend or withdraw the audit report and opinion where necessary, with notifications subsequently being sent to the relevant competent authority of establishment for it to review its recognition of the cloud computing service as offering a certain Union assurance level. The information should also enable the same for the relevant competent authority regarding its recognition of the cloud computing service.

(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 supervision of recognised cloud computing service providers. 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

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

(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 activities that concerns public order. The risk assessment should determine which Union assurance level is appropriate for the activities, due to their importance in preserving public order in sectors falling under 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. To ensure consistent application of this Regulation and preserve the integrity of the digital single market, the Commission will provide guidance 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.

(63) In their risk assessments, Union entities and Member State shall assess the sensitivity, criticality and magnitude of personal and non-personal data processed in cloud environment. 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 on the mapping between Union assurance levels and categories of information, taking into account the sensitivity, criticality and magnitude of the data processed by the cloud environment, the systematic importance of the activities of the contracting authorities, and the applicable obligations arising from Union law. 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.

(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.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.

(65) To enhance resilience and limit dependency on a single cloud computing service provider, Union entities and Member States should, as part of their public procurement procedures, consider whether a multi-vendor or multi-cloud strategy may be appropriate. The decision to adopt and implement a multi-cloud architecture should be based on a context-specific risk assessment. The assessment should identify any relevant operational, regulatory or resilience-related circumstances that would support the adoption of a multi-vendor or multi-cloud strategy.

(66) Public procurement frequently serves as a primary signal of market direction. Requirements imposed by or on public authorities to adopt specific assurance levels offered by cloud computing services tend to be mirrored by private-sector entities operating in regulated industries, with subsequent spillover effects contributing to broader market realignment over time. Those developments underscore the importance of private-sector entities operating in the sectors in Annex I to Directive (EU) 2022/2555 to be able to carry out the same assessments as those carried out by Union entities and Member States.

(67) In public procurement procedures for cloud computing services and AI systems, contracting authorities should include clear European added value as part of the quality evaluation of the tender. Such 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. The criterion relating to European added value should not be decisive for award 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. For this purpose, contracting authorities could consider a maximum weighting of 15 out of 120 points to be allocated to European added value within the overall evaluation methodology, ensuring that it remains proportionate and subordinate to the core contract award criteria.

(68) Innovation procurement in cloud computing services and AI systems is essential to foster technological development, strengthen digital resilience and competitiveness and enable public authorities to benefit from secure, efficient and trustworthy digital solutions that evolve with rapidly changing technological and societal needs. Member States should therefore aspire to award at least 25% of relevant cloud and AI procurement innovation procedures to SMEs. To that end, Member States should actively report on their uptake of innovative cloud computing services and AI systems to the Commission.

(69) In the joint declarations 'Building the next-generation cloud for businesses and the public sector in the EU' of 15 October 2020 ([30]) and the Berlin Declaration on Digital Society and Value-Based Digital Government of 8 December 2020 ([31]), 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 ([32]), 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 national and European cloud initiatives that provide highly trusted and secure public-sector cloud capabilities and facilitate the sharing of such capabilities between Union entities and public-sector bodies. 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.

(70) The members of the EuroCloud Federation should comply with specific requirements to avoid any distortion of competition in relation to private economic operators by placing a private provider of services in a position of advantage over its competitors.

---

30 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.

31 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.

32 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.

(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 ([33]), over 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 strategic objectives and significant decisions of the intermediate legal entity that owns the hardware and provides the services. 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.

(72) To ensure effective, secure and resilient provision of services, the sharing entity should put in place appropriate technical, operational and organisational measures. This should include, in particular, policies on risk analysis and information system security, including access control policies, policies on incident handling and business continuity and policies supporting interoperability and connectivity.

(73) Finally, the sharing of data centre services and cloud computing services within the EuroCloud Federation should be anchored in a public-sector cooperation. Such cooperation should be governed solely by considerations of public interest, and should not entail any form of consideration in exchange for another. In particular, the sharing of services within the EuroCloud Federation should be free of charge, except where the charges are limited strictly to what is necessary and proportionate to recover the costs incurred by the sharing entity for the beneficiary using entity. Those costs should be limited to the additional costs incurred in the sharing of capacity, including for allocating and isolating resources, managing access, enabling the integration and interoperability of resources, ensuring compliance with the applicable requirements under Union law and managing the sharing relationship. The fees levied by the sharing entity to recover those costs should not be deemed as a consideration for the provision of a service and should not constitute a pecuniary interest or public contract within the meaning of Directive 2014/24/EU of the European Parliament and of the Council ([34]) and Regulation (EU, Euratom) 2024/2509. Under those conditions, the sharing of public-sector data centre services and cloud computing services within the EuroCloud Federation should not fall under Union public procurement rules.

(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. 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

---

[33] 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).

[34] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

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, 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.

(75) In order to increase flexibility and administrative efficiency, it is appropriate to provide, in a derogation from the Regulation (EU, Euratom) 2024/2509, for the possibility of adding participating entities during the lifespan of a dynamic purchasing system. Under that derogation, participating entities that have acceded to the agreement after the establishment of a dynamic purchasing system should be permitted – subject to the prior approval of the Commission – to join that system at any point during its period of validity, before any future invitation to tender is issued. That possibility should be strictly limited to newly acceding participating entities and should not affect the rights and obligations of entities already participating in the system or the integrity of procurement procedures already concluded or ongoing.

(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. 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.

(77) Where participating entities enter into an agreement for the provision of central purchasing activities, including ancillary purchasing activities, they should not apply the public procurement procedures provided for in applicable Union law, in accordance with Directive 2014/24/EU and Regulation (EU, Euratom) 2024/2509. Any contracting authority from Member States entering into such an agreement for the purpose of organising central purchasing activities should be deemed to fulfil its obligations pursuant to the national law transposing Directive 2014/24/EU if it purchases works, supplies or services from a contracting authority responsible for the procurement procedure.

(78) The agreement should establish a steering committee composed of the Commission and representatives of Member States. The committee is 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. 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 stages of autonomous conduct. 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.

(80) In order to ensure that the necessary resources remain available, the participating entities will 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. 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.

(81) Open source plays an important role in ensuring transparency, security and efficiency in the use of digital technologies by the public sector. Access to the source code enables auditability, fosters collaboration and reuse and reduces dependency on a single vendor, thereby limiting the risk of vendor lock-in. Promoting the use of open source is therefore essential to support innovation, ensure better value for public expenditure and strengthen the Union's digital autonomy. In that context, the choice of cloud computing services or software has significant implications not only for cost-efficiency, but also for security, interoperability, accountability and technological autonomy

(82) To ensure the efficient, transparent and interoperable use of digital technologies across the Union's public sector, it is necessary for public administrations to promote open standards and components released under an open source licence when building their cloud and AI ecosystem or stack.

(83) An increasing number of Union entities and public-sector bodies are sharing software developed by or for them and making it available for reuse under an open-source licence. This may be considered to be in the public interest and may maximise the

value of public expenditure, reduce duplication costs and foster innovation across the Union. However, software is often made available and accessible in different repositories or catalogues, hampering searchability, discoverability and, ultimately, reuse. It is therefore necessary to require Union entities and public-sector bodies that voluntarily decide to make software available for reuse to do so in a catalogue or repository that is connected to EU Open Source Solutions Catalogue ('the EU OSS Catalogue'). The OSS Catalogue should serve as a centralised catalogue for any public administration to search and access software made available for reuse by Union entities and public sector bodies. Hosting the EU Open Source Solutions Catalogue on the Interoperable Europe portal referred to in Article 8 of Regulation (EU) 2024/903 ([35]) will ensure that solutions can be easily linked to further relevant information and training.

(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') bringing together 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.

(85) In order to take account of technological development and maintain an efficient framework of measures for strengthening the cloud and AI ecosystem at Union level, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of: amending Annex I to reflect relevant market and technological developments regarding the Cloud and AI Leadership Initiatives and amending Annex II to update the criteria for Union assurance levels; supplementing this Regulation by laying down detailed rules for the performance of audits; amending Annex III; specifying a Union assurance level for a contracting authority; and requiring an impact assessment and risk mitigation measures for private companies operating in sectors of high criticality.

(86) When adopting delegated acts under this Regulation, it is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level, and that those consultations are conducted in accordance with the principles set out in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([36]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should always have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(87) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should

---

35 Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

36 Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making (OJ L 123, 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj).

be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([37]).

(88) Due to the relevance of this Regulation on the protection of personal data, the European Data Protection Supervisor should be consulted, where necessary, in accordance with Article 42(1) of Regulation (EU) 2018/1725 ([38]).

(89) If any of the measures provided for by this Regulation constitute State aid, the provisions concerning such measures are without prejudice to the application of Articles 107 and 108 TFEU.

(90) This Regulation should be without prejudice to the application of Articles 101 and 102 TFEU, and to the enforcement powers of competition authorities.

(91) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States, but can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the TEU. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

HAVE ADOPTED THIS REGULATION:

---

37 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, (OJ L 55, 28.2.2011, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

38 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

TITLE I
GENERAL PROVISIONS

Chapter I
Subject matter and definitions

Article 1
Subject matter

1. This Regulation establishes a framework for strengthening the cloud and AI ecosystem at Union level, in particular through the following measures:
   (a) establishing the Cloud Leadership Initiative and the AI Leadership Initiative (‘the Cloud and AI Leadership Initiatives’);
   (b) setting the framework for the accelerated deployment of data centres across the Union;
   (c) enabling the availability of a sovereign cloud and artificial intelligence (AI) offer to safeguard the Union’s public order;
   (d) reducing dependencies on critical technologies;
   (e) fostering the adoption of cloud computing services across the public sector.
2. The first general objective of this Regulation is to ensure the conditions necessary for the competitiveness and innovation capacity of the Union’s cloud and AI ecosystem.
3. The second general objective, separate from and complementary to the first general objective in paragraph 2, is to improve the functioning of the single market by laying down a uniform Union legal framework for increasing the Union’s resilience and strategic autonomy in cloud and AI technologies.

Article 2
Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘cloud computing service’ means cloud computing service as defined in Article 6, point (30), of Directive (EU) 2022/2555;

(2) ‘cloud computing service provider’ means a legal entity which provides a cloud computing service;

(3) ‘AI system’ means an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689;

(4) ‘frontier AI’ means AI models or AI systems built upon such models that can perform a wide variety of tasks and that approach, reach or exceed the current state of the art;

(5) ‘AI agent’ means an AI system or a coordinated set of AI systems, that can perceive and act upon their environment, with a degree of autonomy, using tools as needed to achieve specific goals and adapt to changing inputs and contexts;

(6) ‘public sector body’ means public sector body as defined in Article 2, point (1), of Directive (EU) 2019/1024;

(7) ‘Union entities’ means the Union institutions, bodies, offices and agencies set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of the European Union (TFEU) or the Treaty establishing the European Atomic Energy Community;

(8) ‘small and medium-sized enterprise’ or ‘SME’ means a small or medium-sized enterprise as defined in Article 2 of Annex I to Commission Recommendation 2003/361/EC;

(9) ‘small mid-cap’ or ‘SMC’ means a small mid-cap enterprise as defined in point 2 of the Annex to Commission Recommendation (EU) 2025/1099;

(10) ‘data centre’ means data centre as defined in point 2.6.3.1.16 of Annex A to Regulation (EC) No 1099/2008 of the European Parliament and of the Council;

(11) ‘data centre operator’ means data centre operator as defined in Article 2, point (7), of Delegated Regulation (EU) 2024/1364;

(12) ‘data centre service’ means data centre service as defined in Article 6, point (31), of Directive (EU) 2022/2555;

(13) ‘software’ means software as defined in Article 3, point (4), of Regulation (EU) 2024/2847;

(14) ‘hardware’ means hardware as defined in Article 3, point 5, of Regulation (EU) 2024/2847;

(15) ‘component’ means component as defined in Article 3, point (6), of Regulation (EU) 2024/2847;

(16) ‘manufacturer’ means manufacturer as defined in Article 3, point (13), of Regulation (EU) 2024/2847;

(17) ‘auditing organisation’ means an individual organisation, a consortium or other combination of organisations, including any subcontractors, that the audited cloud computing service provider has contracted to perform an independent audit;

(18) ‘audited service’ means a cloud computing service being audited for the purpose of receiving an audit report and an audit opinion;

(19) ‘audit criteria’ means the criteria, pursuant to Annex II to this Regulation, against which the auditing organisation assesses whether the audited provider and its audited service comply with each cumulative criterion to be met for it to be recognised as offering Union assurance levels 2, 3, or 4;

(20) ‘audit evidence’ means any information used by an auditing organisation to support the audit findings and conclusions and to issue an audit opinion, including data collected from documents, databases or IT systems, interviews or testing performed;

(21) ‘control’ means control as defined in Article 2, point (6), of Regulation (EU) 2021/697;

(22) ‘contracting authorities’ means contracting authorities as defined in Article 2(1), point (1), of Directive 2014/24/EU;

(25) ‘open source licence’ means open source licence as defined in Article 2, point (12), of Regulation (EU) 2024/903.

TITLE II
RESEARCH, DEVELOPMENT AND DEPLOYMENT ACTIVITIES FOR THE CLOUD AND AI ECOSYSTEM

Chapter I
Cloud and AI Leadership Initiatives

Article 3

General objective of the Cloud and AI Leadership Initiatives

1. The Cloud and AI Leadership Initiatives shall pursue the general objective of promoting research and innovation activities and achieving large-scale capacity throughout the Union's cloud and AI ecosystem, by:

   (a) supporting the development and deployment of cutting-edge cloud and AI technologies, including next-generation resource-efficient data centre technologies, open cloud computing stack technologies, frontier AI, and physical and industrial AI;

   (b) reinforcing the Union's data centre and cloud capacity to meet the growing demands driven by AI, foster innovation and ensure the resilience of the digital infrastructure;

   (c) stimulating the Union's demand and promoting the deployment and uptake of cloud and AI technologies across the public sector, and the private sector, in line with the digital target of digital transformation of businesses, established by Decision (EU) 2022/2481.

2. The Cloud and AI Leadership Initiatives shall pursue the following operational objectives:

   (a) supporting the development and deployment of advanced data centre technologies incorporating principles of energy efficiency and resource efficiency by design and throughout operations (operational objective 1);

   (b) supporting the development and deployment of cloud computing stacks supporting the Union's technological autonomy (operational objective 2);

   (c) advancing Union's capabilities in frontier AI (operational objective 3);

   (d) advancing Union's capabilities in physical AI models and systems and fostering their deployment across the Union's strategic sectors (operational objective 4);

   (e) accelerating the development and uptake of industrial AI across the Union's strategic sectors (operational objective 5);

   (f) supporting the development of advanced platforms for the large-scale deployment of AI agents (operational objective 6);

   (g) increasing the development and adoption of AI models and systems across the Union's public sectors (operational objective 7);

(h) increasing the adoption of AI technologies at regional and local level, and the uptake of cloud computing services provided by European cloud computing service providers (operational objective 8).

Article 4

Operational objectives of the Cloud and AI Leadership Initiatives

1. Under operational objective 1, the Cloud and AI Leadership Initiatives shall:

   (a) advance energy- and water-efficiency technologies for data centres, including innovative cooling, next-generation direct current data centres, waste heat utilisation solutions, and energy storage systems;

   (b) promote the integration of emerging quantum computing technologies for cloud and AI computing infrastructure operations;

   (c) develop AI-powered technologies for optimising server efficiency, utilisation rates and computing infrastructure operations;

   (d) design and optimise cloud and edge AI infrastructures to ensure effective integration with energy grids and to increase theirflexibility;

   (e) leverage data centres as anchor clients for advanced energy management systems harnessing diverse energy sources, including small modular reactors and clean hydrogen, alongside efficient energy storage solutions;

   (f) deploy test beds and pilot lines to integrate and test technologies developed under points (a) to (e), covering energy-efficient semiconductor and quantum computing prototypes.

2. Under operational objective 2, the Cloud and AI Leadership Initiatives shall:

   (a) develop and pilot secure, resilient and performant open cloud computing stacks covering on-device edge, connectivity, data and AI tools, backend and service layers for strategic sectors;

   (b) develop AI-optimised servers and baseline software based on processors, accelerators and quantum accelerators designed and manufactured in the Union, alongside next-generation ultra-high density and long-term data storage;

   (c) boost data availability for AI via open-source middleware platforms underpinning common European data spaces;

   (d) foster the creation of open-source software foundations supporting open-source components;

   (e) establish a catalogue of European open cloud computing solutions developed under points (a) to (d) of this paragraph.

3. Under operational objective 3, the Cloud and AI Leadership Initiatives shall support pioneering projects in frontier AI that develop frontier AI models and systems as strategic assets, including in key sectors such as cybersecurity.

4. Under operational objective 4, the Cloud and AI Leadership Initiatives shall:

   (a) accelerate the development of a European physical AI stack, supporting model training and system development and deployment, in particular for robotics and autonomous vehicles and drones;

(b) facilitate access to, and the collection and preparation of, specific datasets for physical AI;

(c) support the development, testing and validation in real-world environments of physical AI models and systems.

5. Under operational objective 5, the Cloud and AI Leadership Initiatives shall:

(a) accelerate the development and uptake of sectoral AI models and systems across the Union's strategic industrial sectors;

(b) facilitate access to the necessary computing resources and AI tools required to develop and operationalise AI models and systems tailored to industrial sector needs;

(c) enable secure large-scale data pooling for collaborative AI training through technologies enhancing privacy and preserving confidentiality.

6. Under their operational objective 6, the Cloud and AI Leadership Initiatives shall:

(a) support the development of advanced resilient and secure platforms for the development, deployment and orchestration of advanced AI agents at scale;

(b) facilitate the development of targeted testing and experimentation methodologies of advanced AI agents and their orchestration throughout their lifecycle.

7. Under operational objective 7 the Cloud and AI Leadership Initiatives shall:

(a) accelerate the technological development and uptake of AI models and systems in critical public sector domains;

(b) develop AI models and systems that increase the effectiveness of public service delivery and accessibility for the general public, improve decision-making, and simplify administrative procedures;

(c) promote the sharing and reusing of training data and AI models across the Union's public services;

(d) facilitate secure, privacy-enhancing health data reuse for AI models and tools in healthcare;

(e) facilitate the development, testing and deployment of AI models and tools in the automotive sector, including for autonomous driving.

8. Under operational objective 8 the Cloud and AI Leadership Initiatives shall:

(a) promote the broad adoption of AI by private and public sector organisations, including SMEs and SMCs, through the network of Experience and Acceleration Centres for AI ('Centres for AI');

(b) develop a common cloud and AI curriculum, drawing on the network of Centres for AI and other relevant European initiatives;

(c) promote the sharing of public sector data centre services and cloud computing services by supporting a European public sector cloud federation ('EuroCloud Federation');

(d) support the procurement of data centre services and cloud computing services for Union entities and public sector bodies.

Article 5

Experience and Acceleration Centres for AI

1. Each Member State shall establish Experience and Acceleration Centres for AI ('Centres for AI'). Those Centres for AI shall build on the European digital innovation hubs established under Article 16 of Regulation (EU) 2021/694 and, where applicable, any successor entities established under Union law.

2. The objectives of the Centres for AI shall be to:

   (a) support the integration and scaling-up of AI use cases in strategic industrial and public sectors;

   (b) accelerate the broad adoption of cloud and AI technologies at regional and local levels, notably for SMEs, SMCs and public sector bodies, in line with the 'AI first' principle;

   (c) leverage relevant infrastructure to accelerate the development and fine-tuning of AI models and systems.

3. The Centres for AI shall be tasked, in particular, with:

   (a) helping organisations accelerate their digital transformation through access to and use of AI technologies, including by connecting organisations with European providers of cloud and AI technologies;

   (b) ensuring or providing access to relevant upskilling and reskilling schemes, in close collaboration with the AI Skills Academy;

   (c) facilitating the transfer of expertise across regions;

   (d) supporting the scaling-up of spin-offs and start-ups emerging from universities, incubators and other accelerators by facilitating access to clients, companies and organisations seeking specialised AI services.

4. The Commission may adopt implementing acts detailing the procedure for establishing Centres for AI and further arrangements concerning the participant organisation profile, selection criteria and details on the implementation of the tasks and functions. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).

5. Centres for AI shall have substantial overall autonomy as regards their organisation, composition and working methods, in compliance with the objectives set out in this Regulation.

6. A network of Centres for AI shall be established to support collaboration and the exchange of best practices among Centres for AI, and to provide specialised services across regions where the required skills or compute capacity are not available locally.

7. Member States and the Commission shall cooperate with existing networks established under other Union initiatives, including Union initiatives in the field of semiconductors and data.

Article 6

Implementation of the Cloud and AI Leadership Initiatives

1. The implementation of the Cloud and AI Leadership Initiatives' operational objectives shall be entrusted to the Commission and the Member States and, where

relevant, to joint undertakings or any other structures capable of achieving those objectives.

2. The Cloud and AI Leadership Initiatives' operational objectives shall be implemented through large-scale, cross-sectoral initiatives addressing major technological and industrial challenges of strategic relevance for the Union ('grand challenges'), as indicated in Annex I.

3. The Cloud and AI Leadership Initiatives may be supported by funding from Union programmes, including Horizon Europe and the Digital Europe Programme, in accordance with Regulation (EU) 2021/694 and Regulation (EU) 2021/695.

4. To reflect technological and market developments the Commission is empowered to adopt delegated acts in accordance with Article 45 to amend Annex I in a manner consistent with the objectives of the Cloud and AI Leadership Initiatives set out in Article 4.

Article 7
National cloud and AI strategies

1. By [same day as entry into force plus one year], Member States shall establish national cloud and AI strategies (the 'national strategies').

2. The national strategies shall include at least the following:

   (a) key objectives and priorities for cloud and AI adoption, in line with the 'AI first' principle, as well as a governance and monitoring framework to achieve those objectives and priorities;

   (b) measures to accelerate the development and adoption of cloud and AI at national, regional and local level, particularly among public sector bodies, SMEs and SMCs, including by supporting the Centres for AI referred to in Article 5 as entry points to the European AI innovation ecosystem;

   (c) measures to support the broad deployment and uptake of AI in strategic industrial and public sectors, including in healthcare, energy and mobility;

   (d) measures to support the deployment of data centre capacity, with a particular focus on high-value data centres delivering significant economic and societal benefits while adhering to high environmental and energy-efficiency standards;

   (e) measures to invest in high-intensity computing infrastructure, including AI factories, AI gigafactories and quantum computers as strategic national and cross-border assets supporting research, development and industrial AI deployment across strategic sectors;

   (f) measures to support the development of cloud and AI capabilities and promote excellence and innovation, including through public procurement measures, and public procurement of innovation measures set out in Article 33;

   (g) measures to support the development of cloud computing stack technologies built upon open hardware and software to strengthen technological sovereignty and enhance the competitiveness of strategic European industries;

   (h) measures to ensure the accessibility of high-quality data for AI development, notably by preventing data bottlenecks encountered by organisations.

3. National strategies shall be consistent with the objectives of this Regulation

4. Member States shall ensure that their national strategies are consistent with, and contribute to, the associated digital targets established under Article 4 of Decision (EU) 2022/2481.

5. The Member States shall notify the Commission of their national strategies within three months of their adoption. Member States shall assess their national strategies at least every three years on the basis of key performance indicators and, where necessary, update them. The Commission shall monitor the adoption and revision of the national strategies.

6. The European Artificial Intelligence Board established by Regulation (EU) 2024/1689 (the 'AI Board') shall advise and assist the Member States as regards the coordination of national strategies. The AI Board shall facilitate exchange of best practices among Member States.

Article 8

Criteria for frontier AI priority projects

The Commission may, by means of a decision, recognise as frontier AI priority projects, projects selected through open calls for expression of interest that support grand challenge 3 set out in Annex I, provided that the following criteria are fulfilled:

(a) it is a pioneering project, focused on the support and scaling-up of frontier AI technologies;

(b) it is undertaken by a European digital infrastructure consortium established pursuant Decision (EU) 2022/2481 or another legal entity eligible for funding under Union law and it involves the participation of at least three Member States;

(c) the participating Member States pool computing time and other relevant resources to support the implementation of the designated project.

Article 9

Computing support for AI projects

1. The Union and the Member States shall ensure that sufficient AI computing resources from their compute capacities are allocated to support the development of frontier AI priority projects that fulfil the criteria set out in Article 8, within the limits of available capacity.

2. The Union shall at least match the AI computing resources contributed by Member States to frontier AI priority projects to the extent that sufficient AI computing capacity is available within the Union's share of European high performance computing access time.

3. The Union and the Member States shall endeavour to provide sufficient computing resource for AI industrial innovation, physical AI and public sector AI projects.

TITLE III
DATA CENTRE CAPACITIES

Chapter I
Data centre acceleration zones

Article 10

Designation of data centre acceleration zones

1. Where data centre capacity is being deployed within the territory of a Member State, that Member State shall designate at least one data centre acceleration zone ('acceleration zone') within its territory by [P.O. insert the date of entry into force of this Regulation plus 6 months]. Member States shall consider the following aspects when designating acceleration zones:

   (a) the location and dimension of the site or area, and the minimum and maximum size of the facilities that could be built on that site or area;

   (b) the available and future power grid capacity and the possibility and conditions for on-site storage and clean energy generation;

   (c) the available and future network connectivity capacity;

   (d) the capacity of the zone to support the phasing out of legacy copper networks;

   (e) the available and future facilities that can reuse data centre waste heat;

   (f) all the measures taken to accelerate the granting of the necessary permits for constructing and operating data centres within the given zone;

   (g) the preference for reusing brownfield sites over using greenfield sites;

   (h) the ability of the site or area to function sustainably, particularly as regards preventing or minimising environmental impacts and supporting the reduction of carbon emissions and its climate resilience.

2. Member States, where appropriate to facilitate the development of acceleration zones, shall:

   (a) conduct, and review at least every three years, a comprehensive analysis of the energy needs and their respective impacts on greenhouse gas emissions, of current and future acceleration zones and identify the required energy infrastructure capacity for the proper functioning and development of data centre projects located in the acceleration zones. Such analysis shall be conducted, at least, when designating the acceleration zones pursuant to paragraph 1;

   (b) ensure that the network development plans prepared by transmission system operators pursuant to Article 51 of Directive (EU) 2019/944 of the European Parliament and of the Council and distribution system operators pursuant to Article 32 of Directive (EU) 2019/944 take due account of the analysis prepared pursuant to point (a) of this paragraph, considering the potential of anticipatory investments to accommodate future system needs.

3. National, regional and local authorities responsible for preparing spatial and development plans shall consider including, in those plans, provisions for the

development of data centre projects deployed in acceleration zones, and of the necessary infrastructure. Member States shall ensure that all relevant spatial planning data are available to data centre operators. Where those plans are subject to an assessment pursuant to Directive 2001/42/EC of the European Parliament and of the Council and Article 6 of Directive 92/43/EEC, those assessments shall be combined. Where applicable, the combined assessment shall also address the impact on potentially affected water bodies referred to in Directive 2000/60/EC of the European Parliament and of the Council.

4. When designating acceleration zones, Member States shall ensure the involvement of and coordination among all relevant national, regional and local authorities and entities, including operators as defined in Article 2, point (29), of Directive (EU) 2018/1972 of the European Parliament and of the Council, transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944 and distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944.

Article 11
Conditions within acceleration zones

1. When setting sustainability requirements for data centres deployed in acceleration zones, Member States shall use the key performance indicators specified in Delegated Regulation (EU) 2024/1364 pursuant to Directive (EU) 2023/1791 under Annex II, from (a) to (n).

2. Member States shall ensure that the allocation and use of resources within acceleration zones takes place on fair, reasonable and non-discriminatory terms and does not give rise to speculative reservation or foreclosure practices capable of impeding effective competition or the effective development or use of those zones.

Article 12
Single information points

1. The data centre operator shall have the right, upon request, to be assisted by a single information point throughout the entire lifecycle of the data centre project in an acceleration zone with respect to all authorisations required for the deployment of the data centre. For that purpose, Member States shall designate one or more single information points for data centre operators of data centre projects in acceleration zones. The Member States may designate for this purpose a single information point established under Regulation (EU) 2024/1309. The functions, procedures and mechanisms applicable to such single information points under Regulation (EU) 2024/1309, including those relating to digital access, administrative coordination and dispute settlement, shall also apply.

2. The role of a single information point may include, among other things, coordinating, facilitating, monitoring and sharing information on the procedure relating to:

   (a) spatial planning and building permits;

   (b) environmental assessments, in accordance with Regulation (EU) 2026/XXXX [on speeding-up environmental assessments];

   (c) authorisations regarding water abstraction, wastewater discharge, and heat utilisation and recovery;

   (d) compliance with applicable administrative and reporting obligations;

(e) information to the public, with the aim of increasing public acceptance of the data centre project;

(f) applications for connection to the electricity, heat or communications networks, or to other relevant networks.

3. The single information point shall assist in assessing whether a data centre project may qualify as a strategic project under Article 14.

4. When providing the administrative support and the assistance referred to in this Article, the single point of contact shall pay particular attention to SMEs and, where appropriate, establish a dedicated channel for communication with SMEs to provide guidance and respond to queries related to the implementation of this Regulation.

Article 13

Facilitating administrative and permit-granting processes

1. Data centre projects deployed in acceleration zones shall be considered as strategic projects within the meaning of Article 14 of Regulation (EU) 2026/XXX [on speeding-up environmental assessments] and shall benefit from the toolbox set out in the Annex to that Regulation.

2. For each designated acceleration zone, Member States shall prepare and issue an aggregated baseline permit authorising the deployment of data centres in that acceleration zone. This aggregated baseline permit shall cover the permits and administrative authorisations required for the data centre projects located within the acceleration zone, excluding installation-specific permits.

3. Before issuing the aggregated baseline permit referred to in paragraph 2, Member States shall carry out all necessary procedures and assessments, including any relevant environmental assessments, planning procedures and evaluations applicable at the level of the acceleration zone.

4. Data centres deployed in acceleration zones shall be required to obtain additional permits only for activities falling outside the aggregated baseline permit referred to in paragraph 2.

5. Member States shall ensure that administrative applications related to the planning, construction and the operation of data centre deployed in acceleration zones are processed in an efficient, transparent and timely manner. The permit-granting procedure for data centre projects deployed in data centre acceleration zones shall not exceed 12 months, from the moment a comprehensive application has been submitted. The time limit shall be without prejudice to any shorter time limits set by Member States. Where such a status exists in national law, data centre projects shall be allocated the status of highest national significance possible and be treated as such in permit-granting processes. This paragraph shall apply only where such status exists in national law and shall not create an obligation for Member States to introduce such status.

Chapter II
Strategic projects

SECTION 1
DESIGNATION OF DATA CENTRE STRATEGIC PROJECTS

Article 14
Designation of data centre strategic projects

1. The Commission may, by means of a decision, designate as strategic projects, data centre projects selected through open calls for expressions of interest that fulfil at least two of the following criteria:

   (a) the project establishes and operates infrastructure that directly supports and enhances essential public sector functions, including research and education, healthcare, public safety and security;

   (b) the project includes highly sustainable or innovative features, including technologies and solutions developed under Title II;

   (c) the project contributes to the security, safety, and stability of the electricity grid and contributes to the electricity system needs as evaluated by the relevant system operator, in particular for projects involving the colocation of large clean energy generation and storage facilities;

   (d) the project supports the integration of chips, processors and accelerators, servers or quantum computers designed and/or manufactured in the Union into data centre systems or data centre facility management, thereby strengthening the Union semiconductor, quantum and data centre supply chains and contributing to the objectives of this Regulation and of Regulation (EU) 2023/1781;

   (e) the project addresses a major shortage of compute capacity in an area identified as having such a shortage under Article 15 and contributes significantly to the growth, development and promotion of the local economy.

2. In its proposal, the applicant shall provide all the necessary and relevant information to demonstrate that the project fulfils the relevant criteria.

3. The duration of the designation as a strategic project shall be based on the predicted lifetime of the project. The applicant shall include in the proposal the information necessary to substantiate the predicted lifetime of the project, on the basis of which the duration of the designation as strategic project shall be determined.

4. Where the Commission finds that a project designated as a strategic project no longer fulfils the relevant criteria, or where its designation was based on an application containing incorrect information affecting compliance with those criteria, it may withdraw the designation of that project by means of a decision. Projects for which the designation as a strategic project has been withdrawn shall lose all rights connected to that status under this Regulation.

Chapter III
Monitoring

Article 15
Monitoring the capacity gap

1. For the purpose of monitoring progress in the achievement of the objectives of Decision (EU) 2022/2481, the Commission shall identify and monitor:

   (a) the compute capacity available in the Union, including edge computing capacity;

   (b) the volume of demand for data centre capacity;

   (c) the size of the capacity gap and underserved areas that could be identified by the Commission, in cooperation with the Member States, and subsequently used as acceleration zones for the deployment of data centre capacity.

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 shall meet in order to provide their cloud computing services to Union entities and public sector bodies.

2. 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.

3. To ensure Annex II and Annex III remain up to date with new legal or technical developments, the Commission shall review them at least every 18 months.

Article 17
Recognition of cloud computing service providers

1. A cloud computing service provider that aims to be recognised as offering a Union assurance level, 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.

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 necessary, request one or more competent authorities of the other Member States to collaborate in the procedure for a candidate recognition under this Article. 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 competent authority or refuse the request.

3. For 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 Article 19(2) and all the necessary evidence.

   By way of derogation from the first subpragraph, the EU statement of conformity issued under Article 19(2) by cloud computing service providers that are SMEs shall be directly and automatically recognised in all Member States without the need for prior recognition by the evaluating national competent authority.

4. For Union assurance levels 2, 3 and 4, the candidate 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 evidence provided to the auditing organisation during the audit procedure.

5. Within 60 days of accepting an application pursuant to paragraph 1, the evaluating national competent authority shall assess the 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 for recognition. 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. The evaluating competent authority shall take due account of those comments when finalising its conclusions.

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 shall be deemed accepted by all Member States, the evaluating national competent authority shall adopt the recognition decision and the audited service shall be recognised throughout the Union at the appropriate 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 paragraph 5, point (b) or confirm or modify its original draft decision. Where the requesting competent authority is not satisfied, it may submit a reasoned objection.

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 draft decision. The evaluating national 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 the reasoned objection following the procedure referred to in paragraph 8, whichever is applicable.

10. In case the evaluating national competent authority intends to maintain its draft decision, the concerned national competent authority may refer the matter to the Commission. The Commission shall assess the referral and may request information from the national competent authorities concerned. The Commission shall 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 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).

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 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 18
Associated third countries

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 against the criteria for Union assurance level 3 pursuant to Annex II, provided that that third country fulfils the following cumulative criteria:

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

   (b) it has no measures in place that enable it to exercise control over the 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 Article 32 of Regulation (EU) 2023/2854;

   (c) it has no measures in place to compel the cloud computing service provider 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 has no measures in place to impede the provision of state-of-the-art technologies and services provided by the cloud computing service provider;

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

(f) the third country grants equivalent levels of access to public procurement procedures of cloud computing services 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 third country no longer fulfils the requirements under paragraph 1, the Commission shall repeal, amend or suspend the decision referred to in paragraph 1.

3. The Commission shall publish on its website a list of third countries that fulfil the requirements under paragraph 1 and those that no longer do so.

SECTION 2
CONFORMITY ASSESSMENT PROCEDURES

Article 19
Conformity self-assessment

1. Cloud computing service providers seeking recognition in accordance with Article 17 as offering Union assurance level 1, shall carry out a conformity self-assessment of 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 compliance with the criteria for Union assurance level 1 have been demonstrated. By issuing such a statement, the cloud computing service provider shall assume responsibility for the compliance of the cloud computing service with the criteria for Union assurance level 1set out in Annex II.

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

SECTION 3
INDEPENDENT THIRD-PARTY AUDITS

Article 20
Independent audit

1. Cloud computing service providers seeking recognition in accordance with Article 17 as offering Union assurance level 2, 3, or 4, 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 necessary 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.

4. Audits referred to 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 period before the beginning of the audit;

      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;

   (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 revoke its audit report and audit opinion where the audited provider, intentionally or negligently, supplied incorrect or misleading audit evidence.

8. 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.

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 in the central repository and shall remain available there for five years.

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

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 cloud computing service provider shall, 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 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 needs to be amended or revoked. 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 penalties provided for shall be effective, proportionate and dissuasive. Member States shall, as soon as possible, notify the Commission of those rules and of those measures and shall notify the Commission of any subsequent amendment affecting them.

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

   (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.

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 providers of their obligations under this Chapter.

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.

Article 26
Powers of the national competent authorities

1. Where needed to carry out their tasks under Article 17, 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;

   (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, 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, including with any of the investigative orders issued pursuant to paragraph 1;

(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 may request other competent authorities to provide specific information in their possession relating to a specific cloud computing service provider 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.

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 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 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 the competent authority of establishment considers that the information provided is insufficient, it may either request additional information. The period set out in paragraph 4 shall be suspended until that additional information is provided

4. The competent authority of establishment shall, as soon as possible 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 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, that contribute to the preservation of public order in sectors falling under Annex I or II of 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;

   (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.

2. In carrying out their risk assessments, Member States and Union entities shall consider at least the following aspects:

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

   (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. 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 Member States use the highest level of assurance for the most critical public sectors activities 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.

5. If the Commission concludes, after reviewing the results of the risk assessment or assessments of a Member State, 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, the Commission may adopt implementing acts in accordance with Article 46(2) specifying the Union assurance levels needed for the public sector activity.

6. Where the risk assessment requires the migration to another cloud computing service, the Member State or Union entity shall migrate within a reasonable transition period that shall not exceed 12 months, taking into account technical feasibility, continuity of service and data portability requirements applicable to such migration.

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.

Article 30

Public procurement

1. This Article applies to contracting authorities that procure cloud computing services for their exclusive use. Without prejudice to Article 136 of Regulation (EU, Euratom) 2024/2509, this Article also applies to Union entities that procure cloud computing services for their exclusive use.

2. Union entities and public sectors bodies whose public sector activities have not been identified as contributing to the preservation of public order under the risk assessment referred to in Article 29(1) shall use cloud computing services that have been recognised under Article 17 as having a Union assurance level 1.

3. Contracting authorities, including the 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 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, shall only procure cloud computing services that have been recognised as having a Union assurance level 2, 3 or 4.

4. By derogation from paragraphs 2 or 3, on an exceptional basis and where duly justified, contracting authorities 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 cannot be supplied by recognised cloud computing services available in the central repository referred to in Article 22, and no adequate or reasonable alternative or comparable cloud computing service exists, and such absence is not the result of an artificial narrowing down of the parameters of the public procurement procedure;

   (b) the contracting authority has launched a similar procurement process within the previous year but did not receive any suitable tenders or suitable participants;

   (a) applying the requirements of this Regulation would require the contracting authority to procure services at disproportionate cost.

SECTION 2
PRIVATE SECTOR ENTITIES

Article 31

Impact assessments

1. Entities referred to in Annex I of Directive (EU) 2022/2555 who are not public sector bodies may carry out similar assessments as those set out in Article 29.

2. The Commission may issue guidance on the methodology for carrying out the impact 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 AI systems, 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.

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 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 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 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, 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.

Article 33
Monitoring of procurement of innovation in cloud and AI

1. 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 inform the Commission, on a yearly basis, of the following information:

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

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

   (c) measures taken to improve SMEs access to public procurement procedures.

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

5. Union entities and contracting authorities shall promote:

   (a) preliminary market consultations;

   (b) matchmaking between public buyers and innovative solutions provided by European SMEs and start-ups;

   (c) development of public contract clauses that are favourable for innovative SMEs.

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 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;

4. The Commission is empowered to adopt implementing acts to specify the procedure to participate in the EuroCloud Federation and template 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 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 through which the service is made available and provides the service that is made available to the using entity. Where the sharing entity indirectly owns the hardware and provides the services through an intermediate legal entity, the sharing entity shall exercise control over that intermediate legal entity.
2. The sharing entity shall put in place appropriate technical, operational and organisational measures to ensure an effective, secure and resilient provision of services.
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 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.
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.
6. The Commission is empowered to adopt implementing acts to specify the technical, operational and organisational measures referred to in paragraph 2. 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.
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 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).

Chapter IV
Procurement of data centre services, cloud computing services, software and AI systems 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 for itself and forUnion entitiesand 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.

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 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 intended for the participating entities;

   (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 services, cloud computing services, software and AI systems;

(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.

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.

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 mandate referred to in Article 168(2) and (3) 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 decision-making process for the choice of procedure and the applicable conditions, 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 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.

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 before it is launched by the Commission, to ensure its compliance with the framework established by this Regulation.

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.

8. The Steering Committee shall set transparent and non-discriminatory 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, 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.

10. The Steering Committee may make accession to the agreement conditional on participating entities accepting one or more ancillary support services, 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 from the Commission as a central purchasing body 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.

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.

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.

   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, and other relevant, duly justified objective criteria.

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 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.

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.

TITLE V
FINAL PROVISIONS

Article 44
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 6(4), Article 16(2), Article 20(9), Article 21(1), and Article 31(3) shall be conferred on the Commission for an indeterminate period of time from [date of entry into force].

3. The delegation of power referred to in Article 6(4), Article 16(2), Article 20(9), Article 21(1), and Article 31(3) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. Delegated act adopted pursuant to Article 6(4), Article 16(2), Article 20(9), Article 21(1), and Article 31(3) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 46
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 47
Review

1. By [date of entry into force plus 4 years], and every 5 years thereafter, the Commission shall evaluate this Regulation, and report to the European Parliament, the Council and the European Economic and Social Committee.

2. Where appropriate, the report referred to in paragraph 1 shall be accompanied by a proposal for amendment of this Regulation.

3. In carrying out the evaluation referred to in paragraph 1, to Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources, and shall pay specific attention to small and medium-sized enterprises and the position of new competitors.

Article 48

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [same day and month as date of entry into force plus 1 year].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE 3
1.1. Title of the proposal/initiative 3
1.2. Policy area(s) concerned 3
1.3. Objective(s) 3
1.3.1. General objective(s) 3
1.3.2. Specific objective(s) 3
1.3.3. Expected result(s) and impact 3
1.3.4. Indicators of performance 3
1.4. The proposal/initiative relates to: 4
1.5. Grounds for the proposal/initiative 4
1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative 4
1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone. 4
1.5.3. Lessons learned from similar experiences in the past 4
1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments 5
1.5.5. Assessment of the different available financing options, including scope for redeployment 5
1.6. Duration of the proposal/initiative and of its financial impact 6
1.7. Method(s) of budget implementation planned 6
2. MANAGEMENT MEASURES 8
2.1. Monitoring and reporting rules 8
2.2. Management and control system(s) 8
2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed 8
2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them 8
2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure) 8
2.3. Measures to prevent fraud and irregularities 9
3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE 10
3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected 10

3.2. Estimated financial impact of the proposal on appropriations 12
3.2.1. Summary of estimated impact on operational appropriations 12
3.2.1.1. Appropriations from voted budget 12
3.2.1.2. Appropriations from external assigned revenues 17
3.2.2. Estimated output funded from operational appropriations 22
3.2.3. Summary of estimated impact on administrative appropriations 24
3.2.3.1. Appropriations from voted budget 24
3.2.3.2. Appropriations from external assigned revenues 24
3.2.3.3. Total appropriations 24
3.2.4. Estimated requirements of human resources 25
3.2.4.1. Financed from voted budget 25
3.2.4.2. Financed from external assigned revenues 26
3.2.4.3. Total requirements of human resources 26
3.2.5. Overview of estimated impact on digital technology-related investments 28
3.2.6. Compatibility with the current multiannual financial framework 28
3.2.7. Third-party contributions 28
3.3. Estimated impact on revenue 29
4. DIGITAL DIMENSIONS 29
4.1. Requirements of digital relevance 30
4.2. Data 30
4.3. Digital solutions 31
4.4. Interoperability assessment 31
4.5. Measures to support digital implementation 32

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act).

Short title: The Cloud and AI Development Act (CADA)

(Text with EEA relevance)

1.2. Policy area(s) concerned

The proposal concerns policy areas linked to the development of cloud computing services, with a focus on ensuring a smooth and timely transition toward high-value, resilient and future oriented digital ecosystems. It aims to set the regulatory conditions for a Single Market in cloud computing services, incentivising investment in cloud infrastructure, AI research and development and supporting emerging requirements arising from innovative technologies. By modernising existing frameworks, the initiative aims to facilitate efficient investment, promote sustainable competition, and reduce technological dependencies, thereby supporting the EU's long-term competitiveness and resilience in the global cloud and AI landscape. The proposal also aims to remove persisting barriers to the cross-border provision of cloud computing services and improve regulatory coherence and predictability across Member States.

1.3. Objective(s)

1.3.1. General objective(s)

The general objective of this initiative is to ensure the functioning of the internal market for cloud computing services and to secure the conditions necessary for the Union's competitiveness and strategic autonomy**.**

1.3.2. Specific objective(s)

Specific objective No 1: Increase computing capacity deployed in the EU through innovative and sustainable technologies. By 2030, the EU should at least triple its current data centre capacity, prioritising energy-efficient technologies in new installations. As demand continues growing, this should be considered an intermediate objective so that by 2035, the computing capacity in the EU should meet its needs.

Specific objective No 2: Ensure attractive conditions for the deployment of sustainable and innovative computing capacity. While the first objective is aimed at the deployment of capacity, this one targets the conditions for such investment and deployment. By 2030, operators should be able to obtain all permits to build and run a data centre in less than 18 months throughout the EU, including access to land, permits for energy access, and connectivity, which are a major attention point for investors.

Specific objective No 3: Decrease the overall reliance on non-European cloud computing services. By 2035, this intervention should increase the market share of European cloud computing service providers in the European market. Strengthening the Union's strategic autonomy requires reducing dependencies and ensuring that

European users have credible European alternatives to non-European incumbents. A stronger European supply base improves the Union's capacity to act autonomously and enhances long-term resilience, competitiveness, and security of supply.

Specific objective No 4: Contribute to the protection of public order by enhancing the resilience of supply of cloud computing services, in particular in the public sector. By 2035, highly critical use cases in the public sector should be operated using sovereign cloud and AI computing services to ensure data confidentiality, operational autonomy and prevent harms that could undermine public order. Highly critical use cases are those of particular systemic importance that underpin essential functions or involve the processing of sensitive data. Ensuring that, for these, data is protected, and service continuity is guaranteed, is a key element of attaining strategic autonomy. That is why these use cases are a priority for the move towards services whose provision is outside of the reach of third-country policies that could result in data access or interruptions to service continuity, i.e. sovereign services.

1.3.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The proposed Cloud and AI Development Act is expected to have a relevant impact on several beneficiaries, including the public sector, the European cloud and AI ecosystem and citizens. The initiative aims to strengthen the cloud and AI ecosystem at Union level, pioneering energy and resource efficiency for data centres, develop European open cloud and AI stacks, and promote the uptake of cloud computing services. This is expected to lead to the development of advanced AI technologies and frontier AI, the acceleration of industrial AI models and systems in strategic sectors, and the support of cross sectoral initiatives addressing major technological and industrial challenges. Furthermore, the proposal seeks to accelerate data centre deployment across the Union, tripling the EU's data centre capacity within the next five to seven years and ensuring the deployment of resource-efficient data centres. The Act also aims to promote autonomy, reduce dependencies on critical technologies and increase the adoption of cloud computing services across the public sector, enabling critical sectors to use sovereign cloud computing services. Additionally, the proposal will lead to the establishment of a European public sector cloud federation, common procurement activities and the promotion of open-source solutions. Overall, the proposal seeks to empower these beneficiairies, fostering a competitive, innovative and autonomous European cloud and AI ecosystem that drives economic prosperity, social wellbeing and strategic autonomy. The proposal is envisioned to have positive effects on the global competitivess of the European AI and cloud sector, and the attractiveness of the EU for third countries' businesses and researchers.

1.3.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Objective 1: Increase computing capacity in the EU through innovative and sustainable technologies.

(a) Installed computing capacity (MW IT load) by MS
(b) Aggregate general purpose and AI-optimised compute, measured also in FLOPs
(c) EU share of global installed computing capacity

(d) Utilisation rate of EU computing capacity; measures on PUE, WUE, location-based emissions and related environmental impact of data centres
(e) Deployment of innovative and energy-efficient technologies (pilots launched and uptake of new solutions)
(f) Share of clean energy in data centres and waste-heat reuse
(g) Total annual public and private investment in EU-based DCs
(h) Share of new data centre capacity deployed outside existing hubs and in underserved regions

Objective 2: Ensure attractive conditions for the deployment of sustainable and innovative computing capacity.
(a) Average permitting time for new data centre projects
(b) Total administrative burden for operators
(c) Share of projects delayed/cancelled due to regulatory or infrastructure barriers
(d) Number of MS with simplified permitting frameworks
(e) Cost competitiveness index

Objective 3: Decrease the reliance on non-European cloud and AI computing services.
(a) Share of total EU cloud computing services revenue captured by European service providers
(b) Number of public sector authorities served by sovereign providers per MS
(c) Share of installed EU DC capacity owned by European providers
(d) Share of idle capacity across MS

Objective 4: Contribute to the protection of public order by enhancing the resilience of supply of cloud computing services, in particular in the public sector.
(a) Number of cloud services audited under levels 2,3,4
(b) Compliance rate by contracting authorities (%) with the sovereignty scheme
(c) Annual value of EU public procurement of sovereign cloud computing services
(d) Number of public sector solutions released as open source in the repository, and their downloads by third parties.

1.4. The proposal/initiative relates to:

☑ a new action

☐ a new action following a pilot project / preparatory action[39]

☐ the extension of an existing action

☐ a merger or redirection of one or more actions towards another/a new action

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The Cloud and AI Development Act will be expected to enter into force within 20 days from the publication in the Official Journal. The entry into application should be within one year of publication, with notable exceptions for rules that require additional transition period.

[39] As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.

1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.

The development of computing capacity in the EU currently takes place along national lines. Each Member State operates under a distinct framework, with different processes and requirements for data centre deployment, reflecting local conditions and needs. However, national policies for data centre acceleration risk further fragmentation and race-to-the-bottom with respect to sustainability. Moreover, an increasing number of low-latency applications require close computing capacity. More generally, the EU faces a shortage of computing capacity, a problem that risks negatively affecting its competitiveness and requires EU-level action to maintain a regulatory and investment environment that is easy to navigate for data centre operators and investors, including across borders.

Closing this capacity gap and allowing European businesses and public administrations to leverage compute capacity while ensuring sustainability requires action at EU level. The dependence on cloud computing services supplied by non-European providers has the same root causes across the EU and affects businesses and public administrations in all Member States. European service providers face difficulties to scale up across the EU, for example due to different national trustworthiness standards, particularly in public procurement. Divergent national procurement practices complexify the market for European providers and the underlying situation of imperfect information is a market failure requiring an EU-level response. Calls for EU-action to address these challenges were also made in the public consultation.

EU action is expected to have a clear added value in addressing the problem of limited and geographically concentrated availability of computing capacity. By providing a common approach to data centre deployment, it would enable the coherent planning and deployment of computing capacity in a geographically balanced way, while avoiding a race to the bottom and reducing regulatory complexity for investors and data centre operators. The EU is uniquely positioned to ensure that investment and acceleration policies reflect collective priorities and avoid fragmentation. EU-level action would ensure that all businesses and public administrations can access sufficient compute capacity to meet their needs and is a prerequisite for Europe to become an AI continent.

In addressing the dependence on cloud computing services supplied by non-European providers, EU action is expected to deliver benefits that exceed what Member States could achieve individually, especially in addressing the underlying market failures of imperfect information. This would improve the functioning of the internal market and enable cloud computing service providers to grow beyond their national markets.

1.5.3. Lessons learned from similar experiences in the past

The proposal is informed by the practical experience in the implementation of existing regulations in this field. Past experience has shown that legal safeguards are needed but not sufficient to change dependence on non-EU providers. GDPR and EDPS enforcement pushed public bodies and providers towards stronger contractual

controls and tighter rules on international transfers. However, these measures produced compliance solutions rather than concrete changes. Similarly, the need for data localisation proved to only partially solve some of the sovereignty requirements needed for specific use cases, especially in the public sector. The EUCS cloud certification preparatory work also demostrated that cybersecurity must be distinguished from sovereignty requirements. The regulation also builds on and complements the Cybersecurity Act 2.0, as well as provisions of the Data Act, which focuses on switching costs, interoperability, portability and unfair contractual terms. Finally, the proposal was informed by an extensive stakeholder consultation strategy.

1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments

The proposal is compatible with the multiannual financial framework as it would primarily provide a new legal framework while relying on existing or planned EU instruments for financing. Its main funding synergies should be with FP10 and the European Competitiveness Fund (ECF), especially under the Digital Leadership window. FP10 should support the upstream research and innovation dimension under Pillar I, while ECF should serve as the main deployment instrument, thus contributing to translate FP10 research outputs into operational capabilities. Other instruments could further reinforce these efforts. IPCEIs would continue to support large-scale, cross-border projects where cloud, edge, chips, cybersecurity or AI infrastructure require coordination among Member States and private invesment. EDICs could provide useful governance vehicles for groups of Member States wishing to jointly operate common digital infrastructure. Cohesion policy instruments, e.g. ERDF and the Cohesion Fund contribute to and may support regional competitiveness and address territorial disparities by co-financing digital infrastructure in less-developed regions. Synergies are also expected with InvestEU by improving the investment environment, supporting bankable projects and complementing financial instruments to mobilise private and public investment. Where relevant, the proposal would also build on reforms and investments set out in national RRPs, including National Reform Programmes and country-specific recommendations. Finally, other ECF policy windows could support sector-specific applications.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The assessment of available financing options has considered both redeployment within existing Commission resources and the need for additional financing. The implementation of the initiative is estimated to require 25 FTEs in total. Of these, 8 FTEs from DG DIGIT and 7 FTEs from DG CNECT are considered to fall within the scope of redeployment, reflecting tasks that can be covered through the reprioritisaton of existing activities and use of existing policy expertise. This means that 15 of the 25 estimated FTEs could be covered through redeployment. These redeployed posts would mainly support activities close to existing mandates, such as policy coordination, legal analysis, stakeholder engagement, internal market monitoring, programme management, administrative support and cooperation with Member States. For the remaining tasks, alternative financing options have been examined. These include targeted reinforcement of relevant budget lines and use of existing programme envelopes. However, given that several tasks may entail significant operational costs, fees are also introduced as an important financing

mechanism and to limit the impact on the EU budget. In particular, such fees had been evisaged to cover activities related to common procurement activities and administration of the EuroCloud Federation for sharing idle capacity among interested Member States.

The remaining 10 FTEs would require additional financing as they related to new or substantially expanded reponsibilities that go beyond current workload assumptions.

Overall, the proposed approach combines redeployment, fee-based financing and limited additional resources. Redeployment would ensure budgetary discipline and use of existing Commission expertise. Fees are expected to reduce pressure on the EU budget and support budget neutrality for most resource-intensive tsasks. Additional appropriations are thus reserved for new functions that cannot be financed through fees or internal reallocation.

1.6. Duration of the proposal/initiative and of its financial impact

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☑ **unlimited duration**

– Implementation with a start-up period from 2028 to 2030,

– followed by full-scale operation.

1.7. Method(s) of budget implementation planned

☑ **Direct management** by the Commission

– ☑ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated

– ☐ international organisations and their agencies (to be specified)

– ☐ the European Investment Bank and the European Investment Fund

– ☑ bodies referred to in Articles 70 and 71 of the Financial Regulation

– ☐ public law bodies

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees

– ☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act

– ☐ bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the controlling bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The Regulation will be reviewed and evaluated five years from its entry into force. The Commission will report on the findings of the evaluation to the European Parliament and the Council. To support the consistent implementation and monitorting of this Regulation, Member States should also ensure that the relevant information concerning their activities is available to the Commission in a timely manner.

2.2. Management and control system(s)

2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation establishes a new policy framework for harmonised rules governing the procurement of cloud computing services in the internal market and the deployment of data centres across the EU, while supporting the Union's policy objectives of consumer trust, industrial competitiveness, security and resilience and sustainability. The Cloud and AI Development Act aims to simplify and improve coordination of the regulatory framework for the development of data centres and procurement of cloud computing services. These objectives require reinforced EU-level coordination and operational capacity, which in turn require targeted and proportionate budgetary resources. The proposal introduces proportionate changes, establishing a governance system with new EU-level tasks with a Single Market dimension, while ensuring that decision-making remains at the most efficient level. The chosen governance model aims to build on existing structures and mandates, thereby limiting the need for new entities and allowing the budget to be implemented through established administrative and financial arrangements, ensuring cost-effectiveness and predictability of expenditures.

In order to carry out these new tasks, additional human resources are required. The implementation and enforcement of the Regulation is estimated to require 6 additional FTEs for the DG CNECT and 4 FTEs for DG DIGIT. The proposed staffing levels are proportionate to the volume and complexity of the new responsibilities and reflect the most cost-efficient option, avoiding duplication at national level.

Payments will follow standard EU budgetary procedures, including commitments and payments made annually, in accordance with the Financial Regulation and within the ceilings of the applicable Multiannual Financial Framework. This will be supported by the annual contributions from the fees covering the costs from additional tasks and long term costs. Expenditure will be subject to the Commission's internal control framework, including ex ante checks, ex post audits, performance monitoring and reporting. This will be performed with the aim to ensure sound financial management, legality and regularity fo expenditure and effective use of Union funds, while ensuring the timely implementation of the Regulation.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The activities proposed in the Act involve different Union entities and some execution risks that require monitoring, oversight, coordination and guidance effort

for their mitigation. The commission will dedicate staff to, among other activities, elaborate guidance documents, delegated acts, dependency assessments, comitology secretariat, and oversight of the implementation of the initiative, including monitoring its progress against established KPIs and milestones. This would allow to promptly identify possible issues and risks in the execution of activities.

In particular for the common procurement activities, a Steering Committee shall be established, composed of the Commission and representatives of Member States, and will be responsible for strategic oversight of the procurement activities, including the strategic orientations of the agenda of public procurement activities, and the strategic orientation of each procurement procedure, ensuring compliance with this Regulation, and transparent and non-discriminatory conditions for accession of contracting authorities. In the case of the European public sector cloud federation, it is important to ensure broad participation from Union entities, while ensuring the highest level of security in the provision of services, in accordance with Union law, to ensure feasibility, effectiveness and continuity. Therefore, it should be open for the participation of voluntary Union institutions, bodies and agencies, as public sector bodies from Member States willing to interconnect their cloud computing infrastructures and deploy interoperable cloud computing services across the Union. The Commission would establish a platform to facilitate the sharing of data centre and cloud computing capacity accessible to its members. Due to the likely criticality and sensitivity of the data and applications hosted in that shared capacity, the platform would include services and mechanisms for secure access and incident management, including shared identity management, mutual authentication tools and incident reporting tools, and capabilities supporting the operation of the provided services, including monitoring of service provision, resource allocation, service activation and performance.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure)

The cost of controls for this initiative have been estimated at Commission level. The source of this information is the Commission's internal management and control system. The costs were estimated based on the staff and resources dedicated to the activities foreseen as part of this initiative. The expected total costs for such controls can be relatively high due to the complexity of the activities proposed and the need for dedicated resources to mitigate execution risks. The control intensity will be adapted to the nature of the expenditure, the type of beneficiaries or contractors foreseen, the amount of financial resources concerned, and the level of risk. Specific actions such as common procurement, EuroCloud Federation, funding management and repository of sovereign services will require specific resources and controls, including strategic oversight, monitoring and incident management. The cost of such controls has been estimated to ensure that it remains proportionate to the value of the funds managed, the complexity of each activity and the identified risks.

In terms of expected error rate, the aim is to maintain this below the 2% threshold. This will be achieved through standard ex ante and ex post controls mentioned above, including e.g. verification of eligibility and legality of expenditure, procurement and contract management checks, monitoring of deliverables, risk-based controls, audits, and recovery procedures where needed. Any deviation from

this would require a coordinated approach and would be discussed on a case-by-case basis.

2.3. Measures to prevent fraud and irregularities

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[40]	from EFTA countries [41]	from candidate countries and potential candidates [42]	From other third countries	other assigned revenue
	MFF headings and budget lines to be determined[43]	Diff./Non-diff.	YES	NO	NO	NO
	Fee revenue (COM will collect the fee)	Diff./Non-diff.	YES	NO	NO	YES

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries and potential candidates	from other third countries	other assigned revenue
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

40 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
41 EFTA: European Free Trade Association.
42 Candidate countries and, where applicable, potential candidates from the Western Balkans.
43 Budget lines for the new MFF are not yet known

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☑ The proposal/initiative requires the use of operational appropriations, as explained below

The amounts indicated below are provisional and remain subject to the final outcome of the 2028-2034 MFF negotiations. This initiative will be financed by redeployment within the operational programmes of the next MFF, and partially by administrative expenditure for staff. At this stage, it is not possible to indicate the contribution from each MFF heading and programme, while it is expected that a significant contribution will come from programmes under heading 2 of the 2028-2034 MFF (e.g. the European Competitiveness Fund, especially under the Digital Leadership window). These estimates have been prepared based on the information currently available and are intended to provide accurate budget estimates.

3.2.1.1. Appropriations from voted budget

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	

DG CNECT			Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**	**POST 2034**	**GRAND TOTAL**
Operational appropriations												
Budget line	Commitments	(1a)	2.386	0.727	2.118	0.427	0.427	0.427	0.427	**6.941**		**6.941**
	Payments	(2a)	1.193	1.557	1.422	1.272	0.427	0.427	0.427	**6.727**	0.214	**6.941**
TOTAL	Commitments	=1a	**2.386**	**0.727**	**2.118**	**0.427**	**0.427**	**0.427**	**0.427**	**6.941**	**0.000**	**6.941**

DG CNECT			Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034	POST 2034	GRAND TOTAL
appropriations for DG CNECT	Payments	=2a	**1.193**	**1.557**	**1.422**	**1.272**	**0.427**	**0.427**	**0.427**	**6.727**	**0.214**	**6.941**

DG DIGIT			Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034	POST 2034	GRAND TOTAL
Operational appropriations												
Budget line	Commitments	(1a)	2.382							**2.382**		**2.382**
	Payments	(2a)	1.191	1.191						**2.382**		**2.382**
TOTAL appropriations for DG DIGIT	Commitments	=1a	**2.382**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**2.382**	**0.000**	**2.382**
	Payments	=2a	**1.191**	**1.191**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**2.382**	**0.000**	**2.382**

From 2029, the VOBU request is the net amount for which the foreseen cloud federation and joint procurement fees have been deducted.

Total (DIGIT + CNECT)	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034	POST 2034	GRAND TOTAL

TOTAL operational appropriations	Commitments	(4)	4.768	0.727	2.118	0.427	0.427	0.427	0.427	**9.323**	0.000	**9.323**
	Payments	(5)	2.384	2.748	1.422	1.272	0.427	0.427	0.427	**9.109**	0.214	**9.323**
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	0	0	0	0	0	0	0	**0**	0	**0**
TOTAL appropriations under HEADING 2 of the multiannual financial framework	Commitments	=4+6	**4.768**	**0.727**	**2.118**	**0.427**	**0.427**	**0.427**	**0.427**	**9.323**	**0.000**	**9.323**
	Payments	=5+6	**2.384**	**2.748**	**1.422**	**1.272**	**0.427**	**0.427**	**0.427**	**9.109**	**0.214**	**9.323**

Heading of multiannual financial framework	4	'Administrative expenditure'

EUR million (to three decimal places)

DG CNECT		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
• Human resources		1.810	1.810	1.810	1.810	1.810	1.810	1.810	**12.670**
• Other administrative expenditure		0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL DG CNECT	Appropriations	**1.810**	**1.810**	**1.810**	**1.810**	**1.810**	**1.810**	**1.810**	**12.670**

DG: DIGIT	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
• Human resources	1.794	1.794	1.794	1.794	1.794	1.794	1.794	**12.558**
• Other administrative expenditure	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**

DG CNECT		Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034
TOTAL DG DIGIT	Appropriations	**1.794**	**1.794**	**1.794**	**1.794**	**1.794**	**1.794**	**1.794**	**12.558**

TOTAL appropriations under HEADING 4 of the multiannual financial framework	(Total commitments = Total payments)	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**25.228**

EUR million (to three decimal places)

		Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034	POST 2034	GRAND TOTAL
TOTAL appropriations under HEADINGS 1 to 4 of the multiannual financial framework	Commitments	**8.372**	**4.331**	**5.722**	**4.031**	**4.031**	**4.031**	**4.031**	**34.551**	**0.000**	**34.551**
	Payments	**5.988**	**6.352**	**5.026**	**4.876**	**4.031**	**4.031**	**4.031**	**34.337**	**0.214**	**34.551**

3.2.1.2. Appropriations covered from fees (EuroCloud and Joint Cloud Procurement)

EUR million (to three decimal places)

Heading of multiannual financial framework			Number									
DG CNECT			Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034	POST 2034	GRAND TOTAL
Operational appropriations financed by fees												
Budget line	Commitments	(1a)	0.000	2.940	4.410	5.880	2.570	2.570	2.570	**20.939**		**20.939**

	Payments	(2a)	0.000	2.940	4.410	5.880	2.570	2.570	2.570	**20.939**		**20.939**
Appropriations of an administrative nature financed by fees												
Budget line		(3)										
TOTAL appropriations	Commitments	=1a+3	**0.000**	**2.940**	**4.410**	**5.880**	**2.570**	**2.570**	**2.570**	**20.939**	**0.000**	**20.939**
for DG CNECT	Payments	=2a+3	**0.000**	**2.940**	**4.410**	**5.880**	**2.570**	**2.570**	**2.570**	**20.939**		**20.939**

DG DIGIT			Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**	**POST 2034**	**GRAND TOTAL**
Operational appropriations financed by fees												
Budget line	Commitments	(1a)	0.000	3.027	4.317	6.037	6.342	6.663	7.001	**33.387**		**33.387**
	Payments	(2a)	0.000	3.027	4.317	6.037	6.342	6.663	7.001	**33.387**		**33.387**
Appropriations of an administrative nature financed from fees												
Budget line		(3)								**0**		**0**
TOTAL appropriations	Commitments	=1a+3	**0.000**	**3.027**	**4.317**	**6.037**	**6.342**	**6.663**	**7.001**	**33.387**	**0.000**	**33.387**
for DG DIGIT	Payments	=2a+3	**0.000**	**3.027**	**4.317**	**6.037**	**6.342**	**6.663**	**7.001**	**33.387**		**33.387**

			Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**	**POST 2034**	**GRAND TOTAL**
TOTAL operational appropriations	Commitments	(4)	0.000	5.967	8.727	11.917	8.912	9.233	9.570	**54.326**	0.000	**54.326**
	Payments	(5)	0.000	5.967	8.727	11.917	8.912	9.233	9.570	**54.326**		**54.326**

DG DIGIT			Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028-2034	POST 2034	GRAND TOTAL
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)										
TOTAL appropriations under HEADING 2 of the multiannual financial framework	Commitments	=4+6	**0.000**	**5.967**	**8.727**	**11.917**	**8.912**	**9.233**	**9.570**	**54.326**	**0.000**	**54.326**
	Payments	=5+6	**0.000**	**5.967**	**8.727**	**11.917**	**8.912**	**9.233**	**9.570**	**54.326**	**0.000**	**54.326**

3.2.2. Estimated output funded from operational appropriations (not to be completed for decentralised agencies)

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2024**		Year **2025**		Year **2026**		Year **2027**		Enter as many years as necessary to show the duration of the impact (see Section1.6)						**TOTAL**	
	OUTPUTS																	
	Type[44]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[45]…																		
- Output																		
- Output																		
- Output																		

44 Outputs are products and services to be supplied (e.g. number of student exchanges financed, number of km of roads built, etc.).

45 As described in Section 1.3.2. 'Specific objective(s)'

Subtotal for specific objective No 1																	
SPECIFIC OBJECTIVE No 2 ...																	
- Output																	
Subtotal for specific objective No 2																	
TOTALS																	

3.2.3. Summary of estimated impact on administrative appropriations

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below

3.2.3.1. Appropriations from voted budget

VOTED APPROPRIATIONS	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL 2028 - 2034
HEADING 4								
Human resources	3.604	3.604	3.604	3.604	3.604	3.604	3.604	**25.22Ff8**
Other administrative expenditure	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal HEADING 4	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**25.228**
Outside HEADING 4								
Human resources	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 4								
TOTAL	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**3.604**	**25.228**

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.3.2. Appropriations from external assigned revenues

Not applicable.

3.2.3.3. Total appropriations

See table above.

3.2.4. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources

– ☑ The proposal/initiative requires the use of human resources, as explained below

3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)

VOTED APPROPRIATIONS	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034
• Establishment plan posts (officials and temporary staff)							
20 01 02 01 (Headquarters and Commission's Representation Offices)	11	11	11	11	11	11	11
20 01 02 03 (EU Delegations)	0	0	0	0	0	0	0
01 01 01 01 (Indirect research)	0	0	0	0	0	0	0

01 01 01 11 (Direct research)		0	0	0	0	0	0	0
Other budget lines (specify)		0	0	0	0	0	0	0
• External staff (inFTEs)								
20 02 01 (AC, END from the 'global envelope')		14	14	14	14	14	14	14
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY]	- at Headquarters	0	0	0	0	0	0	0
	- in EU Delegations	0	0	0	0	0	0	0
01 01 01 02 (AC, END - Indirect research)		0	0	0	0	0	0	0
01 01 01 12 (AC, END - Direct research)		0	0	0	0	0	0	0
Other budget lines (specify) - Heading 7		0	0	0	0	0	0	0
Other budget lines (specify) - Outside Heading 7		0	0	0	0	0	0	0
TOTAL		**25**	**25**	**25**	**25**	**25**	**25**	**25**

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.4.2. Financed from external assigned revenues

Not applicable.

3.2.4.3. Total requirements of human resources

The staff required to implement the proposal (in FTEs):

	To be covered by current staff available in the Commission services	**Exceptional additional staff***		
		To be financed under Heading 7 or Research	**To be financed from BA line**	**To be financed from fees**
Establishment plan posts	5	6	N/A	
External staff (CA, SNEs, INT)	10	4		

* The estimated impact on expenditure and staffing for 2028 and beyond is indicative and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and annual budgetary procedure and the steering mechanism.

Overall, 15 FTEs requested for the initiative are already in place and will be redeployed with the following repatriation:

– DG CNECT: 2 FTEs in establishment plan posts and 5 FTEs in external staff

– DG DIGIT: 3 FTEs in establishment plan posts and 5 FTEs in external staff

In addition to these existing resources, the initiative requires 10 FTEs of exceptional additional staff. These consist of 6 officials and 4 contract agents and have the following split between DG CNECT and DG DIGIT:

– DG CNECT: 3 FTEs in establishment plan posts and 3 FTEs in external staff

– DG DIGIT: 3 FTEs in establishment plan posts and 1 FTE in external staff

These are requested on top of the current staffing levels to ensure full and effective implementation of the initiative. The new tasks introduced by the proposal cannot be absorbed by the respective DGs' existing human resources. The additional human resources required for this proposal cannot be covered by redeployments within the DG/service or from redeployments from the limited Commission redeployment pool.

Description of new tasks to be carried out by DG CNECT and DG DIGIT:

Officials and temporary staff	Official and temporary staff will be tasked to: 1. Determine and manage the Work Programmes under Pillar 1 of the initiative, including the development of detailed project plans, budgets, resource allocation, KPIs and monitoring mechanisms. 2. Produce guidance documents, delegated acts, dependency assessments, comitology secretariat, and oversee the implementation of the initiative, including: a. Development of comprehensive guidelines, recommendations, templates and tools to support Member States in their implementation efforts on Pillar 2 and Pillar 3 of the initiative b. Development of implementing acts, where needed, e.g. on the requirements applicable to the members of the EuroCloud Federation and the procedure to assess their application c. Drafting market monitoring reports to identify cloud computing services where the Union has a high level of dependence on a single or limited number of third country legal entities for such services d. Providing secretariat services including the development of documents and reports, coordination with stakeholders e. Monitoring progress of the initiative against the established KPIs and milestones, identifying possible issues and risks and providing technical assistence and support to Member States as needed f. Establishment of a knowledge management system to capture and share best practices, lessons leadrned and expertise across the initiative 3. Draft tender specifications for an external provider to build, develop and maintain the repository of sovereign services, and evaluate and determine subsequent governance procedures. After setup, regularly audit/assess a sample of certified services, which are part of the repository, including the development of audit protocols and assessment methodologies and/or quality control procedures to ensure the reliability of the information provided. 4. Procure the EuroCloud Federation platform and support the setup of the federation. Manage the governance mechanisms of the federation, e.g. certification of requirements for membership in the federation, evaluation of applications from Member States and other public sector bodies to join the federation, development and enforcement of common rules and policies for participation in the federation. 5. Setting up systems not currently in place, as part of the joint procurement framework, including managing the complexity of AI procurement, relationships with Member States and contracting authorities and ensuring that the framework is effective and efficient. This will include tasks such as, setting up and managing the procurement processes for cloud, software, and AI systems, coordinating with participating organisations and service providers, managing the contracts and agreements with service providers, ensuring compliance with EU regulations and policies.

	6. Develop and maintain relationships with stakeholders, including Member States, industry representatives, and other relevant parties, to ensure that the initiative is well-coordinated, effective, and responsive to the needs of its stakeholders, including the organisation of regular meetings, workshops, and conferences to facilitate communication and collaboration. This would also include close cooperation with competent authorities on investigative and enforcement measures to ensure compliance with Title IV of the Act.
External staff	External staff will be tasked to: 1. Regularly manage the projects awarded under Pillar 1 work programmes, including the monitoring of their progress, coordination with beneficiaries, and verification of project deliverables and milestones to ensure they are delivered on time, within budget and with the required quality standards. The initiative will be implemented in the next MFF and will build on the results of existing projects already approved under Horizon Europe and the Digital Europe Programme, e.g. Simpl and the Smart Networks and Services Joint Undertaking, including in coordination with other Units. 2. Establish and operate support mechanisms to provide guidance to Member States for the deployment of data centre acceleration zones, particularly during the first two years of the initiative. This will involve the provision of ad hoc support to Member States as they develop and implement their national strategies and plans. After the initial period, this will transition to a more ad hoc coordination role, focusing on providing targeted support to Member States as needed, and ensuring that the initiative remains aligned with the needs and priorities of its stakeholders. 3. Set up and manage a study each year to monitor the computing capacity across Europe, including setting out the scope and methodology of the study, verifying the data collected, reviewing deliverables. 4. Manage the joint procurement activities, in particular in relation to strategic sourcing and market shaping, i.e. vendor management office and drafting of specifications and technical requirements for cloud, AI and software services. 5. Manage the repository of sovereign services on a yearly basis, including by overseeing the contractor activities related to the repository's operations, including technical project management, i.e. ensuring that the contractor delivers the repository according to the agreed technical specifications, timelines, and budget, while also monitoring the contractor's processes to ensure that the repository meets the required standards. 6. Manage the external contractor covering the administrative, technical and operational activities of the EuroCloud Federation platform each year, as well as the technical aspects of the EuroCloud Federation platform, including oversight of technical architecture and infrastructure.

3.2.5. Overview of estimated impact on digital technology-related investments

Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

Exceptionally, when required for the implementation of the proposal/initiative, the appropriations under Heading 7 should be presented in the designated line.

The appropriations under Headings 1-6 should be reflected as "Policy IT expenditure on operational programmes". This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 "Digital dimensions".

TOTAL Digital and IT appropriations	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL MFF 2028 - 2034
HEADING 4								
IT expenditure (corporate)	0	0	0	0	0	0	0	**0**
Subtotal HEADING 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Outside HEADING 4								
Policy IT expenditure on operational programmes	0	0	0	0	0	0	0	**0**
Subtotal outside HEADING 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ☑ can be fully financed through redeployment within the relevant heading of the multiannual financial framework (MFF)

Without prejudice to the negotiations on the next MFF, the appropriations allocated to the Cloud and AI Development Act related activities from 2028 onwards will be covered via redeployments from ECF under the 2028-2034 MFF and partially from fees.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation

– ☐ requires a revision of the MFF

3.2.7. Third-party contributions

The proposal/initiative:

– ☑ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	Total
Specify the co-financing body								
TOTAL appropriations co-financed								

3.3. Estimated impact on revenue

– ☐ The proposal/initiative has no financial impact on revenue.

– ☑ The proposal/initiative has the following financial impact:

– ☐ on own resources

– ☐ on other revenue

– ☑ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[46]						
		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Joint Cloud Procurement service fee (DG DIGIT)		0.000	3.027	4.317	6.037	6.342	6.663	7.001
Cloud Federation fee (DG CNECT)		0.000	2.940	4.410	5.880	2.570	2.570	2.570

For assigned revenue, specify the budget expenditure line(s) affected.

Joint Cloud procurement service fee:

The assigned revenue will be used to cover the budget expenditure linked to the brokerage system put in place for the Joint Procurement scheme. The revenue will be allocated to support the operational costs of the system, including the costs of external staff, tools, and systems.

The breakdown of the assigned revenue will be on average as follows: around 50% will be allocated to cover operational and administrative costs, e.g. studies and research to inform procurement decisions, community management tools and systems to support communication and collaboration among participating organisations, technical enablers and platform integration; around 30% will be allocated to cover the costs of developing and maintaining the necessary tools and systems, such as procurement platforms and marketplaces, contract life-cycle management systems, portfolio and demand management tools; around 20% will be allocated to cover the costs of additional specialised external staff, e.g. for software procurement, data protection activities, Back-office, FinOps and ContractOps to manage contractual aspects, portfolio and demand management.

This allocation aims to ensure that the assigned revenue is used to cover only the operational costs of the system and the budget expenditure linked to the brokerage system. These costs will be allocated based on effective demand needs, ensuring that the resources are used efficiently to support the Joint Procurement scheme.

Cloud Federation Fee:

[46] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20% for collection costs.

The assigned revenue will be used to cover the budget expenditure linked to the services and platform put in place for the EuroCloud Federation. The revenue will be allocated to support the operational costs of the system, including the costs of external staff, tools, and systems.

The expenditure required to finance the federation consists of operational and development-related costs. A significant share relates to the development and maintenance of the platform. Development costs are expected to be highest during the first years, reflecting the initial deployment phase. From year 4 onwards, costs would cover ongoing operations, technical support and periodic upgrades. The maintenance contract would include quality assurance and performance assessment carried out by an external contractor, estimated at around 10% of the total procurement value, based on similar procurement contracts. Operational costs include the cost of external technical experts (10 profiles) on top of the internal FTEs which would be responsible for coordination and project management (see above under the description of new tasks to be carried out by DG CNECT). Their involvement would ramp up progressively, with approximately 40% of capacity in year 1, 80% in year 2, and reaching full capacity from year 3 onwards, in line with the increasing operational needs of the federation. Further expenditure includes IT infrastructure costs, such as hosting services and security-related tooling, which are necessary to ensure the reliability, scalability and protection of the platform.

This allocation aims to ensure that the assigned revenue is used to cover the operational costs of the system and the budget expenditure linked to the services provided. These costs will be allocated based on effective demand needs, ensuring that the resources are used efficiently to support the EuroCloud Federation. Initial establishment costs may be borne by the general budget of the Union and reimbursed by the participating authorities over a defined period through the fees.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

Joint Cloud procurement service fee:

The fee is meant to cover the operational costs for the procurement activities (interinstitutional procurement, joint procurement and central purchasing activities) and the possible ancillary procurement activities.

The payers of the fee would be participating contracting authorities. The fee would increase the price for contracting authorities. However, this will be set in a way to cover only the necessary costs for administering the procurement activities, as the objective of this common procurement would be to be able to negotiate better conditions, lower prices for all contracting authorities and facilitating the adoption at scale of technologies that evolve constantly.

The fees are calculated pro-rata per transaction or via a flat fee per subsequent awarded contract, as specified in the procurement document. The fees will be computed based on a yearly forecast of the beneficiaries' consumption and will be perceived yearly before the execution of the contracts. The fees charged to the participating contracting authorities shall not exceed the verifiable costs incurred by the Commission. It shall be recomputed each year, proportionally to the volume of work foreseen and costs incurred. The starting data of collection of the fee would be 2029, to allow for an initial setup process. The fee will be collected through existing

online services for invoicing and collecting payments from participating contracting authorities.

Projected annual revenue depends on both the number of participating authorities (beneficiaries) and their average expected purchases. The fee revenue will need to reach approximately EUR 6 million per year to cover the forecast average annual costs. Based on estimates on participation, it should be reachable with an average annual fee rate of 2% applied to the spending per authority. If total spending exceeds this level, e.g. because more authorities participate, average spending per authority is higher, or both, the fee rate would decrease proportionately. Revenue from the fee will be used to finance the entire operational costs of the procurement mechanism, explained above.

The Commission shall report to the European Parliament and the Council on the overall amount of the costs incurred for the procurement activities and the total amount of the fees charged.

Cloud Federation fee:

The fee is meant to cover the operational costs for establishing and managing the EuroCloud federation, including assessing membership applications and facilitating the sharing of data centre services and cloud computing services through the development of the EuroCloud Federation platform.

The payers of the fee would be members of the federation. The fee would slightly increase the overall costs for participants. However, it shall be calibrated strictly to cover the essential administrative and operational costs of running the federation. This is expected to create efficiencies and cost savings. By enabling members to exchange capacity and make use of otherwise idle resources, participants can access services at more favourable rates than those available on the open market. This shared model can reduce the need for external procurement and improve overall resource utilisation, especially in the short to medium term. While the fee introduces a marginal cost, it is balanced by the economic benefits derived from collaboration, improved capacity usage and more competitive pricing within the federation.

The Commission shall adopt implementing acts laying down detailed rules relating to determining the fees to be levied by the Commission, specifying the estimated costs attributable to the activities for which fees are chargeable, the individual fee amounts chargeable, as well as the ways and conditions under which the fees should be paid.

The membership fee would be structured as a cost-recovery mechanism, proportionate to the number of participating entities in the federation. The goal is to cover costs while progressively reducing the financial burden on each member as participation increases.

The uptake is assumed to grow over time, with approximately 20% of possible entities joining in the first year, 40% in the second year, 60% in the third year, around 80% in year 4 before achieving full participation in the fifth year. The first year would be dedicated to setting up the federation so no full membership fee would apply. Based on the estimations done, from year 2 onward, the membership fee could be set at around EUR 75 000 per member, reflecting the relatively low number of participants. As more entities join and the cost base is shared across a larger group, the fee could gradually decrease and reach around EUR 30 000 per member once full capacity is achieved. The scheme is expected to reach a break-even point around year 4. At that stage, the fee structure would stabilise at a level sufficient to sustain

operations without generating considerable surplus, in line with the cost-recovery principle.

The starting data of collection of the fee would be 2029, to allow for an initial setup process. The fee will be collected through online services for invoicing and collecting payments from participating authorities.

The estimated annual revenue would depend on the number of participating members and the applicable membership fee. Based on an average membership fee of around EUR 75 000 per member, annual revenues would reach around EUR 4.4 million per year to cover the forecasted average annual operating costs of the federation, including the initial fixed costs. As participation increases, the costs of administering the federation would be distributed across a larger number of members. Consequently, the fee per member would decrease proportionately, with annual revenues stabilising at a lower level, e.g. of around EUR 2.6 million per year.

The Commission shall report to the European Parliament and the Council on the overall amount of the costs incurred for the federation activities and the total amount of the fees charged. The period for reporting is still to be determined.

The use of assigned revenue for the joint procurement and EuroCloud federation offers a budgetary policy opportunity to ensure a dedicated and stable funding stream for these initiatives. By earmarking the revenue from the fee for specific purposes, the Commission can guarantee that the funds are used efficiently and effectively to support the development of a European cloud ecosystem. This approach is justified by the need to provide a clear and predictable financial framework for both initiatives under CADA, which will allow to plan and implement them in a strategic and long-term manner.

In terms of compliance with the budgetary principles of universality and unity, the use of assigned revenue is justified by the fact that these initiatives are designed to support specific and clearly defined policy objectives, i.e. the development of a European cloud ecosystem for sharing idle capacity among Member States and the joint procurement of cloud services to achieve efficiencies and economies of scale. The revenues from the fees will be used to finance specific items of expenditure that are directly related to the achievement of these objectives, as specified above in the respective sections covering both activities. By using assigned revenue, the Commission can ensure that the funds are used in a targeted and efficient manner, without affecting the overall balance of the Union's budget. Furthermore, the use of assigned revenue is consistent with the principle of unity, as it will enable the Commission to implement these initiatives in a coherent and coordinated manner, avoiding duplication of efforts and ensuring that the funds are used to support a common European objective. The Commission will also ensure that the use of assigned revenue is transparent and accountable, with regular reporting and evaluation of the initiative's progress and impact.

In addition, the Commission will take into account the need to avoid any potential distortions or inequalities in the treatment of different cloud service providers, and will ensure that the use of assigned revenue is fair, proportionate, and non-discriminatory. The Commission will also consult with relevant stakeholders to ensure that the initiative is designed and implemented in a way that is responsive to their needs and concerns.

It is important to note that only the operational costs of the two initatives, as outlined above, will draw on the assigned revenue generated by the fees. Administrative costs, on the other hand, will not be covered by the assigned revenue.

In the event that the fees do not materialise in the amount and timing assumed, the Commission has taken a cautious approach to mitigate the risks. In the case of joint procurement, if the fees do not materialise, it would mean that no system would be put in place, and the initiative would not incur any significant costs. On the other hand, the EuroCloud Federation builds on pre-existing studies and current evidence of Member State interest in this initiative. Moreover, the major costs associated with the initaitive are already covered under the current Multiannual Financial Framework under the budget already assigned to the Commission, which altogether reduces this financial risk. Overall, this approach will allow the Commission to adjust its plans, without incurring significant financial risks and be more flexible to adapt its resource allocation as needed, in order to ensure the success of these initiatives.

4. DIGITAL DIMENSIONS

4.1. Requirements of digital relevance

High-level description of the requirements of digital relevance and related categories (data, process digitalisation & automation, digital solutions, and/or digital public services).

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
TITLE II RESEARCH, DEVELOPMENT AND DEPLOYMENT ACTIVITIES FOR THE CLOUD AND AI ECOSYSTEM *Article 7 National cloud and AI strategies*	Member States shall **notify the Commission of their national strategies**.	European Commission National competent authorities	Notification	Data
TITLE III DATA CENTRE CAPACITIES *Article 14 Designation of data centre strategic projects*	**Applications for designation of data centre strategic project shall provide all the necessary and relevant information** to demonstrate that the project fulfils the relevant criteria.	Project operators European Commission	Application insights monitoring	Data

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
TITLE III DATA CENTRE CAPACITIES *Article 15 Monitoring the Capacity Gap*	The Commission shall **monitor** the compute capacity available in the Union, including edge computing capacity; the volume of demand for data centre capacity; the size of the capacity gap.	European Commission National competent authorities	Data collection	Data
TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	A cloud computing service provider that aims to be recognised as offering a Union assurance level, shall **submit an application** for recognition to the national competent authority of establishment.	Cloud computing service providers National competent authorities	Oversight mechanism	Data
TITLE IV AUTONOMY *Article 19 Conformity self-assessment*	The cloud computing service provider **may issue a conformity self-assessment** to demonstrate compliance with Union assurance level 1**. These are to be made publicly available**.	Cloud computing service providers National competent authorities European Commission	Oversight mechanism	Data
TITLE IV AUTONOMY *Article 20 Independent audit*	Establishes the possibility of **independent audits** for Union assurance levels 2, 3, and 4. Provisions related to **data aspects in the context of such audits**.	Cloud computing service providers Auditing organisations European	Oversight mechanism	Data

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
		Commission		
TITLE IV AUTONOMY *Article 21 Content and quality of audit evidence*	**Audits** to be based on Annexes II (Criteria for Union Assurance Levels) and III (Audit evidence for the audit procedure). To be **sufficiently complete and reliable**.	Cloud computing service providers Auditing organisations European Commission	Data quality	Data
TITLE IV AUTONOMY *Article 22 Central repository of cloud computing services*	The Commission shall **establish and maintain a dedicated repository of cloud computing services that have received recognition against a Union assurance level.** The **verifying national competent authority of establishment shall register the audited services in the central repository**. Any **revocation of a recognition shall be published, and remain published, in the central register for 5 years**. The **central repository shall be made publicly available by the Commission and regularly updated by the Commission and the national competent authorities of establishment on a dedicated and easily accessible website**.	European Commission National competent authorities	Repository	Digital solution Data Digital public service

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
TITLE IV AUTONOMY *Article 23 Transparency obligations*	On becoming aware of information or material change in circumstances concerning the cloud computing services that may affect the audit report / opinion, the service provider shall without undue delay **notify the auditing organisation and** the national competent authority of establishment. If the results of the audit report and opinion need to be amended or cancelled, the auditing organisation shall without undue delay **notify the national competent authority** and the Commission. If the results of the recognition need to be amended or cancelled, the national competent authority of establishment shall without undue delay **notify the national competent authorities of the other Member States** and the Commission.	Cloud computing service providers Auditing organisations National competent authorities European Commission	Notification	Data
TITLE IV AUTONOMY *Article 24* *Penalties and compensation*	Member States shall notify, as soon as possible, notify to the Commission the rules on penalties and compensation and any subsequent amendment affecting them.	National competent authorities European Commission	Notification	Data

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
TITLE IV AUTONOMY *Article 25 National competent authorities*	Each Member States shall **designate one or more national competent authorities**. Members States shall **notify the list of authorities** to the Commission. The Commission shall **maintain a public register** of the authorities.	European Commission National competent authorities	Designation of competent authorities	Data
TITLE IV AUTONOMY *Article 27 Mutual assistance*	**Data flows** in the context of **cooperation between national competent authorities**.	National competent authorities European Commission	Data exchange	Data
TITLE IV AUTONOMY *Article 89 Cross-border cooperation*	**Data flows** in the context of **cross-border cooperation.**	National competent authorities European Commission	Data exchange	Data
TITLE IV AUTONOMY *Article 29 Risk Assessments*	Member States must **perform a risk assessment or assessments,** taking utmost account of the guidance issued by the Commission. **Member States shall communicate the risk assessment results to the Commission**. For the purpose of the guidance, the **Commission** is entitled to **request information from cloud service providers**.	Member States European Commission Cloud service providers	Risk assessment	Data
TITLE IV	Member States shall **communicate annually to the Commission certain information pertaining to the**	Member States	Reporting	Data

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
AUTONOMY *Article 33 Monitoring of procurement of innovation in cloud and AI*	**monitoring of procurement of innovative** cloud computing services and AI systems.	European Commission		
TITLE IV AUTONOMY *Article 34 Establishment of the European public sector cloud federation*	The Commission shall **establish a platform for the EuroCloud Federation.**	European Commission Union entities Public sector bodies	Requirements for a digital solution	Digital public service Digital solution
TITLE IV AUTONOMY *Article 37 Procurement activities of the Commission*	The Commission may establish and manage a **common procurement platform** including services which may be used for facilitating the performance of the procurement activities under this Chapter.	European Commission	Requirements for a digital solution	Digital solution
TITLE IV AUTONOMY *Article 42 Share and reuse of software*	When making available for reuse under an open-source licence software on which they hold intellectual property rights, a Union entity or public sector body shall **make the software available for reuse on a catalogue or repository that is connected to the EU OSS Catalogue.**	Union entities Public sector bodies European Commission	Catalogue	Digital solution

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level processes	Categories
TITLE IV AUTONOMY *Article 43 EU Open Source Solutions Catalogue*	The **Commission shall provide and maintain an EU Open Source Solutions Catalogue** as a **centralised catalogue to access software made available for reuse by Union entities and public sector bodies** The EU OSS Catalogue **shall be hosted on the Interoperable Europe portal.** The Commission shall **decide on the request of any Union entity or public sector body owning or maintaining a catalogue or repository to connect to and be made accessible through the EU OSS Catalogue**.	European Commission	Catalogue	Digital solution

4.2. Data

High level description of the data in scope

Type of data	Reference to the requirement(s)	Standard and/or specification (if applicable)
Member State National Strategies	TITLE II RESEARCH, DEVELOPMENT AND DEPLOYMENT ACTIVITIES FOR THE CLOUD AND AI ECOSYSTEM *Article 7 National cloud and AI strategies*	Minimum content requirements for the national strategies.
Data related to applications for recognition as a strategic project	TITLE III DATA CENTRE CAPACITIES *Article 14 Designation of data centre strategic projects*	Provide all the necessary and relevant information to demonstrate that the project fulfils the relevant

		criteria.
Statistics and data required for the monitoring of the capacity gap	TITLE III DATA CENTRE CAPACITIES *Article 15 Monitoring the Capacity Gap*	N/A
Data in the context of the submissions of applications by service providers that aim to be recognised as offering a Union assurance level	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	N/A
EU statement of conformity	TITLE IV AUTONOMY *Article 19 Conformity self-assessment*	N/A
Audit report submitted for recognition and related exchanges	TITLE IV AUTONOMY *Article 20 Independent audit* *Article 21 Content and quality of audit evidence*	Data quality: sufficiently complete and reliable; minimum content for audits.
Data on services that receive a recognition	TITLE IV AUTONOMY *Article 22 Central repository of cloud computing services*	The central repository shall contain information of cloud computing services that have been recognised under a specific Union assurance levels
Notification of becoming aware of information or material change in circumstances concerning the cloud computing services that may affect the audit report / opinion / recognition and related data flows	TITLE IV AUTONOMY *Article 23 Transparency obligations*	N/A

Notification of rules and measures on penalties	TITLE IV AUTONOMY *Article 24 Penalties and compensation*	N/A
Data on the designated national competent authorities	TITLE IV AUTONOMY *Article 25 National competent authorities*	N/A
Data used in the context of cooperation between national competent authorities	TITLE IV AUTONOMY *Article 27 Mutual assistance*	N/A
Data used in the context of cross-border cooperation	TITLE IV AUTONOMY *Article 28 Cross-border cooperation*	N/A
Risk assessments performed by Member States	TITLE IV AUTONOMY *Article 29 Risk Assessments*	N/A
Information provided to the Commission by providers for guidance	TITLE IV AUTONOMY *Article 29 Risk Assessments*	N/A
Data pertaining to the monitoring of procurement of innovative cloud services and AI systems	TITLE IV AUTONOMY *Article 33 Innovation procurement*	N/A

Alignment with the European Data Strategy

Explanation of how the requirement(s) are aligned with the European Data Strategy

The proposal is consistent with the rules on switching between data processing services introduced by the Data Act. By enabling switching and removing key sources of vendor lock-in, the Data Act seeks to ensure that cloud service providers in the EU compete on quality, innovation, and price. It seeks to enable cloud users to freely choose the provider that best meets their needs and combine offers of different providers in a multi-cloud approach. However, the Data Act does not contain elements to shape up a more competitive offer of EU cloud services or encourage the entry into the market of a more diverse set of cloud service providers. The Data Act opens the path towards a possible reduction of dependencies on non-EU providers but does not build the road towards a more sovereign and trusted EU cloud computing sector. The cloud switching and interoperability provisions, however, make it possible for users to embrace European cloud computing services more strongly. The Data Act is thus an enabler for the proposal.

Alignment with the once-only principle

Explanation of how the once-only principle has been considered and how the possibility to reuse existing data has been explored

The once-only principle has been duly considered and will systematically be enforced wherever relevant. This is in particular the case for:

(a) The statistics and data required for the monitoring of the capacity gap

(b) The data on services that receive a recognition

(c) The information provided to the Commission for market analysis

Explanation of how newly created data is findable, accessible, interoperable and reusable, and meets high-quality standards

Digital solutions will be provided to ensure the findability, accessibility, interoperability, and reusability of newly created data. Minimum content requirements will promote high-

quality standards for the data.

Data flows

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Member State National Strategies	TITLE II RESEARCH, DEVELOPMENT AND DEPLOYMENT ACTIVITIES FOR THE CLOUD AND AI ECOSYSTEM *Article 7 National cloud and AI strategies*	Member States	European Commission	Within three months of the adoption of a national strategy	Per adoption/ revision
Data related to applications for recognition as a strategic project	TITLE III DATA CENTRE CAPACITIES *Article 14 Designation of data centre strategic projects*	Applicant for designation of a strategic project	European Commission	Application during open calls for expression of interest	//
Data in the context of the submissions of requests by cloud computing services wishing to provide services to Union entities and public sector bodies	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	Requesting cloud computing service provider	National competent authority of their establishment	Request being made to provide services to Union entities and public sector bodies	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Data in the context of the submissions of requests by cloud computing services wishing to provide services to Union entities and public sector bodies: **Outcome of request (reject, ask for additional evidence, recognise the provider's service)**	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	National competent authority	Requesting cloud computing service provider	Conclusion reached on initial recognition	//
Data in the context of the submissions of requests by cloud computing services wishing to provide services to Union entities and public sector bodies: **Distribution of conclusion for review**	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	National competent authority	All national competent authorities	Cloud computing service provider notified of a recognition	//
Data in the context of the submissions of requests by cloud computing services	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service*	All national competent authorities	National competent authority	National competent authority has objections to a conclusion made by a national competent	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
wishing to provide services to Union entities and public sector bodies: **Objections**	*providers*			authority of establishment	
Data in the context of the submissions of requests by cloud computing services wishing to provide services to Union entities and public sector bodies: **Cases referred to the Commission**	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	National competent authorities	European Commission	National competent authorities cannot reach an agreement	//
Data in the context of the submissions of requests by cloud computing services wishing to provide services to Union entities and public sector bodies: **Commission decision on a referred case**	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	European Commission	National competent authorities	Commission reaches a decision on a case where national competent authorities were in disagreement	//
Data in the context of the submissions of	TITLE IV	National competent authorities	European Commission	National competent authorities decide to use	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
requests by cloud computing services wishing to provide services to Union entities and public sector bodies: **Information request**	AUTONOMY *Article 17 Recognition of cloud computing service providers*			their right to an information request	
Data in the context of the submissions of requests by cloud computing services wishing to provide services to Union entities and public sector bodies: **Reply to an information request**	TITLE IV AUTONOMY *Article 17 Recognition of cloud computing service providers*	European Commission	National competent authorities	Information request from national competent authorities received	//
EU statement of conformity	TITLE IV AUTONOMY *Article 19 Conformity self-assessment*	Cloud computing service providers	Public	Self-assessment used	//
Audit report submitted for validation and related exchanges: **information**	TITLE IV AUTONOMY *Article 20 Independent audit* *Article 21 Content and*	Cloud computing service providers	Auditing organisation	Audit being performed	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
required for the audit	*quality of audit evidence*				
Audit report submitted for validation and related exchanges: **audit reports**	TITLE IV AUTONOMY *Article 20 Independent audit Article 21 Content and quality of audit evidence*	Cloud computing service providers	Auditing organisation and national competent authorities	Audit finished	//
Data on services that receive a recognition: **Central repository of cloud computing services**	TITLE IV AUTONOMY *Article 22 Central repository of cloud computing services*	Verifying national competent authority	Central repository of cloud computing services (European Commission)	Recognition granted	//
Data on services that receive a recognition: **Publicly available website provided by the European Commission**	TITLE IV AUTONOMY *Article 22 Central repository of cloud computing services*	European Commission National competent authority of establishment	Public	Recognition granted	//
Notification of becoming aware of information or material change in circumstances concerning the cloud computing services	TITLE IV AUTONOMY *Article 23 Transparency obligations*	Cloud computing service providers	Auditing organisation National competent authority European Commission	Material conditions change on the side of the provider	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
that may affect the audit report / opinion and related data flows: **Initial notification**					
Notification of becoming aware of information or material change in circumstances concerning the cloud computing services that may affect the audit report / opinion and related data flows: **Notification of the audit outcome changing**	TITLE IV AUTONOMY *Article 23 Transparency obligations*	Auditing organisation	National competent authorities (of the establishment and of other Member States) European Commission	Outcome of audit changing	//
Notification of rules and measures on penalties	TITLE IV AUTONOMY *Article 24 Penalties and compensation*	Member States	European Commission	Member States set/amend the framework for imposing penalties	//
Data on the designated national competent authorities: **Notification by**	TITLE IV AUTONOMY *Article 25 National competent authorities*	Member States	European Commission	National competent authorities designated (within a year of date of entry into force)	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Member States					
Data on the designated national competent authorities: **Data in the public register of authorities**	TITLE IV AUTONOMY *Article 25 National competent authorities*	European Commission	Public	National competent authorities designated and Commission notified	//
Data used in the context of cooperation between national competent authorities: **Information Exchange**	TITLE IV AUTONOMY *Article 27 Mutual assistance*	National competent authorities	National competent authorities	Cooperation (exchange of information) between national competent authorities needed	//
Data used in the context of cooperation between national competent authorities: **Requests for assistance (and replies to such requests)**	TITLE IV AUTONOMY *Article 27 Mutual assistance*	National competent authorities	National competent authorities	Assistance deemed necessary	//
Data used in the context of cross-border cooperation: **Request for assessment –**	TITLE IV AUTONOMY *Article 28 Cross-border cooperation*	National competent authorities of a service's destination	National competent authorities of a service's origin	Suspicions of non-compliance giving rise to a request for assistance	//

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
suspicion of non-compliance					
Data used in the context of cross-border cooperation: **Commission informed of suspicions of non-compliance**	TITLE IV AUTONOMY *Article 28 Cross-border cooperation*	National competent authorities of a service's destination	European Commission	A competent authority decide to ask the competent authority of establishment for information to assess suspicions of non-compliance	//
Data used in the context of cross-border cooperation: **Request for assessment – suspicion of non-compliance (Commission)**	TITLE IV AUTONOMY *Article 28 Cross-border cooperation*	National competent authorities of a service's origin	European Commission National competent authorities	Suspicion of noncompliance by other competent authorities or the Commission	//
Data used in the context of cross-border cooperation: **Outcome of a request for assessment – suspicion of non-compliance**	TITLE IV AUTONOMY *Article 28 Cross-border cooperation*	Competent authorities of origin	Requestors European Commission	Within two months of a request being made	//
Risk assessments performed by Member States	TITLE IV AUTONOMY	Member States	European Commission	Risk assessment occurring within one year of entry into force	Bi-annually

Type of data	Reference to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
	Article 29 Risk Assessments				
Information provided to the Commission for guidance	TITLE IV AUTONOMY *Article 29 Risk Assessments*	Cloud service providers	European Commission	//	//
Data pertaining to the monitoring of the procurement of innovative cloud services and AI systems	TITLE IV AUTONOMY *Article 33 Monitoring of procurement of innovation in cloud and AI*	Member States	European Commission	//	Annually

4.3. Digital solutions

Repository of recognised cloud computing services

Digital and/or sectorial policy (when these are applicable)	Explanation on how it aligns
AI Act	Not applicable
EU Cybersecurity framework	The repository will follow cybersecurity best practices of the Commission
eIDAS	The repository will re-use, in so far as relevant, the eIDAS framework
Single Digital Gateway and IMI	Not applicable

Others (e.g., Interoperable Europe Act)	The need for another interoperability assessment under the Interoperable Europe Act (Regulation EU 2024/903) will be evaluated once the operational details for the repository of recognised cloud computing services become available.

EuroCloud platform

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**
AI Act	Not applicable
EU Cybersecurity framework	The platform should include mechanisms for secure access and incident management, such as shared identity management, mutual authentication tools, and incident reporting tools. The platform will follow cybersecurity best practices of the Commission
eIDAS	This will be specified by the Commission at a later stage.
Single Digital Gateway and IMI	Not applicable
Others (e.g., Interoperable Europe Act)	The need for another interoperability assessment under the Interoperable Europe Act (Regulation EU 2024/903) will be evaluated once the operational details for the EuroCloud platform become available.

Common procurement platform

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**

AI Act	Not applicable
EU Cybersecurity framework	The platform will follow cybersecurity best practices of the Commission
eIDAS	This will be specified by the Commission at a later stage.
Single Digital Gateway and IMI	Not applicable
Others (e.g., Interoperable Europe Act)	Not applicable

Catalogue or repository of reusable software that is connected to the EU OSS Catalogue

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**
AI Act	Not applicable
EU Cybersecurity framework	The platform will follow cybersecurity best practices of the Commission
eIDAS	The repository will re-use, in so far as relevant, the eIDAS framework
Single Digital Gateway and IMI	Not applicable
Others (e.g., Interoperable Europe Act)	Not applicable

EU Open Source Solutions Catalogue

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**

AI Act	Not applicable
EU Cybersecurity framework	The platform will follow cybersecurity best practices of the Commission
eIDAS	The catalogue will re-use, in so far as relevant, the eIDAS framework
Single Digital Gateway and IMI	Not applicable
Others (e.g., Interoperable Europe Act)	Article 4 of the Interoperable Europe Act (Regulation EU 2024/903) mandates the share and reuse of interoperability solutions between Union entities and public sector bodies. The EU Open Source Solutions Catalogue delivers upon this requirement.

4.4. Interoperability assessment

Digital public service or category of digital public services	Description	References(s) to the requirement(s)	Interoperable Europe Solutions(s)	Other interoperability solution(s)
Union repository of recognised sovereign services	A dedicated Union repository of cloud computing services that have received recognition. To be established and maintained by the Commission. National competent authorities shall register the relevant services in this repository.	TITLE IV AUTONOMY *Article 22 Central repository of cloud computing services*	//	NA
EuroCloud Federation	Article 34 establishes the European public sector cloud federation (EuroCloud Federation). The EuroCloud Federation should bring together national cloud	TITLE IV AUTONOMY *Article 34 Establishment of*	NA	NA

	initiatives providing highly trusted and secure public sector cloud capabilities and facilitate the sharing of such capabilities between Union entities and public sector bodies. This should be done via a platform accessible to all Federation Members – the EuroCloud Platform.	*the European public sector cloud federation*		

Impact of the requirement(s) as per digital public service on cross-border interoperability

Union repository of recognised sovereign services

Assessment	**Measure(s)**	**Potential remaining barriers (if applicable)**
Alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	The implementation of the Union repository of recognised sovereign services will take utmost account of existing policies and the building blocks stemming from them.	
Organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	The European Commission is tasked with establishing and maintaining the repository. The verifying national authority is responsible for uploading the relevant data into the repository.	The organisational measures will need to be detailed by the Commission, at a later stage.
Measures taken to ensure a shared understanding of the data **Please list such measures**	Semantic measures will be specified by the Commission at a later stage.	

Use of commonly agreed open technical specifications and standards **Please list such measures**	Technical measures will be specified by the Commission at a later stage.	

EuroCloud Federation

Assessment	**Measure(s)**	**Potential remaining barriers (if applicable)**
Alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	The implementation of EuroCloud federation will take utmost account of existing policies and the building blocks stemming from them. In particular: NIS2 for cybersecurity, Simpl, Data Spaces.	NA
Organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	The detailed governance of the Eurocloud platform will be dealt with through secondary legislation.	NA
Measures taken to ensure a shared understanding of the data **Please list such measures**	Semantic measures will be specified by the Commission at a later stage.	NA
Use of commonly agreed open technical specifications and standards	Technical measures will be specified by the Commission at a later stage.	NA

Please list such measures		

4.5. Measures to support digital implementation

Description of the measure	References(s) to the requirement(s)	Commission role	Actors to be involved	Expected timeline
The Commission is empowered to adopt implementing acts specifying (i) the technical, operational and organisational measures and (ii) the procedure to participate in the EuroCloud Federation as referred to in Article 40(2).	Article 40, Article 41	Drafting one or more implementing acts	European Commission Participating Member States	TBD

EUROPEAN
COMMISSION

Brussels, 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

ANNEXES

to the

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

ANNEX I

GRAND CHALLENGES

1. Grand Challenge 1: Environmental sustainability, performance and security of the Union's data centres

Testing and deploying technologies for data centres across the Union to surpass state-of-the-art energy-efficiency and resource efficiency.

This includes achieving lower Power Usage Effectiveness (PUE) and enabling significantly higher server utilisation rates. Examples include:

(1) ***Lowering average Power Usage Effectiveness***: improving the environmental sustainability and performance of the Union's cloud and edge data centres to an average Power Usage Effectiveness (PUE) of 1.15 across the Union. The main focal areas include enabling the development of:

(a) advanced data centre energy efficiency technologies such as cooling, waste heat recovery;

(b) quantum computing technologies for cloud and compute infrastructure operations;

(c) grid integration and advanced energy management systems;

(d) pilot lines for the validation of next-generation energy-efficient technologies at operational scale.

(2) ***Raising average server utilisation rates of data centres:*** raising average server utilisation rates across the Union's data centres towards 50%, by integrating for example, AI-powered technologies for dynamic server utilisation management, runtime workload management and scheduling or for balancing utilisation, energy cost, thermal constraints, and latency requirements.

(3) ***Enhancing the security and resilience of data centres:*** enhancing the security and resilience of data centres' value chain and supply by integrating semiconductor technologies and quantum technologies designed and manufactured in the Union, and by improving their resistance to physical and cybersecurity threats, including targeted attacks.

2. Grand Challenge 2: Cloud stacks

Building end-to-end hardware and software cloud stacks, including AI tools, infrastructure, services and management layers to bridge the Union's critical capacity gaps.

This includes building AI servers powered by semiconductors and quantum technologies designed and manufactured in the Union for distributed and decentralised cloud and edge computing for AI.

Pilot programmes could help demonstrate the capabilities of the European open cloud stacks in strategically important sectors.

3. Grand Challenge 3: Frontier AI

Developing the next generation of multimodal frontier AI models and systems and pioneering novel capabilities.

The focus will be on the architectural design and development of next-generation multimodal models and systems that push the boundaries of current algorithmic capabilities for achieving superior performance in advanced reasoning, cross-modal understanding and agentic

capabilities; investigating novel approaches to model efficiency, cognitive modelling, and alternative computational structures, etc.

The potential applications could include foundational science such as scientific discovery and complex data interpretation, and the development of world models for improved reasoning, automated management simulation and planning.

4. Grand Challenge 4: Physical AI

Developing advanced physical AI models and systems that operate autonomously and safely for delivering robust, manipulation and navigation in unstructured environments.

The focus will be on co-designing software and its underlying hardware architectures and on combining frontier AI techniques with world models supporting physical reasoning for delivering robust manipulation, navigation, and interaction capabilities with minimal human supervision.

The potential applications could include autonomous robots, industrial systems and drones operating in dynamic real-world environments.

5. Grand Challenge 5: Industrial AI

Accelerate the development and deployment of European industrial AI across the Union's strategic sectors.

The focus will be on developing European industrial AI models and systems capable of serving high-value industrial applications. Such models and systems should be adaptable to sector-specific use cases and enable secure deployment.

The initiatives launched under this grand challenge should rely on specialised computing resources and testing facilities necessary to validate AI systems in real-world environments before supporting their large-scale deployment and uptake, including at regional and local level.

In the automotive sector, those initiatives may facilitate the development and deployment of innovative software platforms and AI models for automated driving, while in manufacturing, they may enable the creation of specialised models that optimise production processes. Other strategic sectors that could benefit from industrial AI may include healthcare, energy, agri-food and defence.

6. Grand Challenge 6: Cooperative European Industrial Models

Developing cooperative European industrial AI models and systems for strategic sectors by enabling collaboration at European industrial scale without exposing commercially sensitive data between participants.

The focus will be on advanced confidentiality-preserving technologies. Those mechanisms include federated and distributed training approaches where algorithms are brought to the data rather than data being transferred centrally; secure execution environments, encryption-based processing, anonymisation and pseudonymisation techniques, access compartmentalisation, and protections against the extraction of commercially sensitive information from trained models.

Strategic sectors that could benefit from cooperative European industrial AI models and systems may include aerospace, pharmaceutics, cybersecurity, mobility, autonomous vehicles and drones, energy and defence.

7. Grand Challenge 7: AI Agents Platform

Developing a European AI agent orchestration framework, providing the essential middleware for the resilient and secure deployment of autonomous agents at scale.

The focus will be on (i) exploring innovative technological paradigms that enable multiple AI agents to collaborate effectively, surpassing the capabilities of standalone systems while maintaining rigorous security standards; and (ii) on the creation of resilient, cloud-based open platforms dedicated to the large-scale management of AI agents.

The potential applications could include healthcare (such as clinical decision support and research coordination), cybersecurity (such as threat detection and response), as well as foundational science.

8. Grand Challenge 8: Public Sector AI

Developing AI models and systems, based on high-quality data from the public sector targeting critical domains (such as healthcare, public administration, law and crisis management as well as public services)

The focus will be on public service solutions that are expected to have a high positive impact on the most critical public services and are shared across different levels of public sector organisations.

One target will be to enable data sharing and frontier model development across national public services to increase the impact on the overall Union's public sector, including also in areas handling sensitive data. Privacy-preserving frameworks, (such as federated learning and high-fidelity synthetic data generation), that make it possible to train of models without compromising the confidentiality of underlying datasets, and measures to accelerate the broad uptake of those modems, including at regional and local level, will also help achieve this target.

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. 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.

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 explicitly requires otherwise;

(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 explicitly requires otherwise and at any time, including before, during or after the configuration or use of the service;

(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 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.

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;

(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 explicitly requires otherwise and at any time, including before, during or after the configuration or use of the service;

(d) if the public sector body determines that imposing additional personnel screening and Union citizenship requirements are necessary, the audited provider should ensure that presonnel 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;

(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

(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) 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 that there are no existing laws and practicesin 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 globally 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;

(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 explicitly requires 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, 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 exisit. 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. 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 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 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;

(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) 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;

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 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;

(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 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;

(i) 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.

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.

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 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 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.

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.

(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 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:

(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. 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.

(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.

(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.

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.

(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.

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.

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 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 compunting service provider.*

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 national competent authority 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.

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. 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.

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 auditing organisation should identify and analyse:

(a) all direct and indirect shareholders, up to the ultimate owners;

(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.);

(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);

(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, etc.

(2) The audited provider should request all the above information from its subcontractors and make it available to the auditing organisation.

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;

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.

(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.

(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:

(c) Demonstrating that the Commission has adopted a decision pursuant to Article 19 regarding the third country for which the cloud computing service provider is subject to the control of;

(d) All evidence demonstrating that the audited provider and any subcontractorinvolved 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.

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

(f) 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;

(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;

(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 coutnry 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.

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) evidence that it has identified one or more alternative software solutions, including open-source software. If equivalent software cannot be identified, a solution ensuring minimal viable functionality must be identified. Tests must be implemented and a switchover plan enabling migration to such alternative solutions;

(c) evidence that it can migrate to an alternative solution in the event of any defect or failure of the vendor or restrictions from a third country or a legal entity established in a third country;

(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.);

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;

(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 applied the up-to-date OSS without undue delay;

(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, the audited provider should implement mechanisms to detect and 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 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 the audited provider.

(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 customer data or bypass security procedures.

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