EXPLANATORY STATEMENT

Europe has many of the assets needed to be a leading force in cloud and artificial intelligence: world-class research and talent, a strong industrial base, and a single market of 450 million people. Yet it has not turned these assets into technological leadership, nor into European companies able to grow and scale. Other parts of the world, in particular the United States and China, have been far more successful in building an environment where digital innovation can thrive and translate into tangible economic benefits. In the field of artificial intelligence, the Union has succeeded in setting a legal framework that provides the necessary safeguards around these technologies. It has been far less successful in developing them. A number of European success stories hint at what European businesses can achieve, but they remain the exception rather than the rule. The Cloud and AI Development Act should change that: it should reduce Europe's dependence on a handful of foreign providers and give European companies the room to grow.

The co-rapporteurs are aware that the trajectory of AI remains partly uncertain. There are nonetheless strong indications that it will profoundly affect our societies in all their dimensions: our labour markets and social welfare systems, our cybersecurity, our capacity to innovate and the way our democracies function. These are challenges in which Europe cannot afford to be a bystander.

The co-rapporteurs start from a simple principle: cloud and AI technologies can only be developed in a way that reflects European values and standards if Europe does not merely import technologies built elsewhere, but builds them itself. Rules alone do not create capabilities. The draft therefore places investment, infrastructure deployment and the ability of European businesses to grow at the centre of Europe's cloud and AI strategy.

Democrata

Building those capabilities starts with physical infrastructure. Digital sovereignty requires computing capacity located in the Union, with a growing share of it owned and operated by European companies, and therefore data centres. A sound and healthy development of data centres is the first building block of that strategy: one that respects high environmental standards, is accepted by the communities that host them, and creates genuine value for them.

The lack of technological capabilities in Europe has also created vulnerabilities. Public administrations, critical sectors and businesses have become heavily dependent on a small number of foreign providers. Recent events have shown that access to digital services can be restricted or made conditional for geopolitical reasons, and that data held by foreign providers can fall within the reach of foreign laws. Our critical services must not be exposed to such leverage. The providers on which we rely today remain essential to the functioning of the single market. This Regulation should, however, create the conditions for European players to emerge and scale, so that the benefits of the digital transition accrue to Europeans: quality jobs, greater security and control over their own data.

The Cloud and AI Development Act should therefore give the right signal to attract private capital into European businesses, by creating a predictable market for European sovereign solutions. Investors need demand they can count on; public buyers need solutions they can trust. Predictability and a common European framework are essential to support investment and help European providers scale.

The co-rapporteurs share the objectives the Commission has set for this Regulation. They consider, however, that on several aspects the original proposal would in practice fall short of those ambitions. Their draft report therefore aims to make those objectives more realistically achievable. In doing so, the co-rapporteurs have sought a balance between ambition and workability: between the urgency of building capacity and the need for public acceptance and sustainability, and between a robust sovereignty framework and openness towards the market. On the sovereignty framework, their central choice is one common European standard, rather than 27 national ones. The following sections set out how that balance has been struck in the two main pillars of the proposal.

Data centre capacity: faster procedures, without lowering standards

The co-rapporteurs support the objective of increasing computing capacity in the Union, and in particular sovereign capacity. Closing Europe's capacity gap will require considerable investment, and Europe must remain an attractive destination for capital from all over the world. That expansion must, however, strengthen European players rather than deepen existing dependencies. Permitting delays, fragmented procedures and uncertain grid access are among the main obstacles to that investment. The draft report therefore keeps, and in places reinforces, the acceleration logic of the proposal: integrated spatial planning, combined environmental assessments, single information points and the possibility for data centre projects in acceleration zones to benefit from the toolbox for strategic projects under the forthcoming framework on environmental assessments.

Acceleration must, however, go hand in hand with sustainability and remain compatible with the Union's climate objectives, including climate neutrality by 2050. The co-rapporteurs are conscious of the growing concerns of citizens across Europe about the expansion of data centres and consider them legitimate. Data centres require substantial electricity capacity, while their water use and local impacts vary considerably from one project to another. Their effects on grids, water and land should therefore be assessed project by project. Faster procedures must therefore never mean lower standards: data centres in acceleration zones remain fully subject to Union environmental law, and their expansion must support, not undermine, the decarbonisation of Europe's energy system. Where material impacts are identified, they should be addressed through effective measures, including energy and water efficiency, low-carbon electricity supply, economically and technically feasible waste-heat reuse, and appropriate siting. Sustainability requirements should rely on the key performance indicators already established under the Energy Efficiency Directive and its common rating scheme for data centres, rather than on divergent national criteria, and the uptake of renewable power purchase agreements should be facilitated. These measures connect Europe's digital ambitions with the electricity infrastructure, grid access and low-carbon supply needed to deliver them.

Speed will also only last if it is accepted. Where local communities feel that infrastructure is imposed on them, without being able to contribute meaningfully or to receive the information they need to form an informed judgement, trust is lost, opposition follows and projects are delayed. The co-rapporteurs have therefore built public acceptance into the very design of acceleration zones:

- **Participation before designation.** Local communities should be informed and able to give their views before an area is designated, using existing procedures rather than adding new ones.

Democrata

• **Benefits forhostcommunities.**Regionsidentifiedassuitablesitesshouldbeableto show whatthelocalcommunitystandstogain,suchasinvestment,jobsandservices, and may encouragedeveloperstofindwaystosharebenefitswiththecommunity.

• **Transparency.**Consistentandpubliclyavailablereportingoncapacity,energyand water useisessential,bothtoinformthepublicdebateandtoallowtheUnionto reassess its capacity objectives on the basis of real data, considering applicable legislationontradesecrets.

The co-rapporteursalsowantaccelerationzonestostrengthenEuropeanoperators,including SMEs, while preservinginvestmentopportunitiesandeffectiveuseofavailablelandandgrid capacity. The draftreportthereforegivesEuropeanoperatorsafirstopportunity,foralimited time, to apply forcapacityinaccelerationzones.Capacitythatisnotusedshouldbereleased, so that no one canreservelandorgridconnectionsspeculativelyandprojectsarenotheldback.

The same favourableconditionsshouldapplytotheexpansionandretrofittingofexistingdata centres, and to colocationandedgefacilities,includingthoseoperatedbySMEs.Inthisway, acceleration zones donotbecomeaprivilegereservedforthelargestplayers,butaleverfora diverse European ecosystem.

Finally, building newdatacentresisnottheonlywaytoincreaseEurope'scomputingpower, nor always the fastest.Theco-rapporteursthereforeinvitetheCommissiontoassessinnovative ways of increasing theUnion'scomputingcapacity,suchasthepoolingofexistingcompute resources across MemberStatesandresearchinfrastructures.

Demóerata

The cloud sovereignty framework: one common European standard

The Union cloud sovereignty frameworkisthecoreoftheproposal.Itsvalueliesingiving public buyers, businesses and investorsasingle,crediblereferenceforwhatatrustworthycloud service is. The co-rapporteurs' guidingprincipleisthatthereshouldbeonecommonEuropean standard: one that does not weakenovertime,isnotapplieddifferentlyin27capitals,and cannot be obtained in the most lenientMemberState.

The draft report therefore strengthensharmonisation.Theassurancelevelsshouldestablish harmonised, risk-proportionate requirementsacrosstheUnion.Activitiespresentingequivalent sensitivity and risk should be treatedconsistently,withoutunjustifiednationaldiverging practices. To that end, the co-rapporteurshaveintroducedanon-exhaustivelistofthe categories of activities concerned byeachassurancelevel,whichMemberStatesshouldfollow, departing from it only where the actualsensitivityoftheactivityjustifiesit,andexplaining why. The applicable level should followthesensitivityoftheactivity,regardlessofwhich public sector entity holds the data. Toprevent"auditshopping",assessmentsshouldbecarried out by accredited auditors, on the basisofacommonlistofevidenceandbindingguidance. Those audits should also remain affordable,sothatEuropeanSMEsandstart-upsarenotpriced out of a framework designed to helpthemgrow.

Public procurement is the most powerfultooltheUnionhastocreatealeadmarketfor European cloud providers. Experienceelsewhere,notleastintheUnitedStates,showsthatthe predictability of public contracts canturnpromisingcompaniesintosuccessstories:witha public entity as an anchor customer,theywereabletoinvest,scaleandthenconquerprivate markets. The co-rapporteurs have soughttomakeiteffectivewithoutmakingitunworkablefor contracting authorities. The draft combinesrequirementslinkedtothesensitivityoftheactivity

with targeted derogations where suitable recognisedservicesareunavailableorwouldentail disproportionate cost, subject to safeguardsandreview.

Sovereign resilience cannot stop atthebordersofthepublicsector.ManyofEurope'smost essential services are run by privateoperators:apowerplant,aprivatehospitaloranairportis no less critical because it is privatelyowned.ManycountriesoutsideEuropealreadymakesure that their most critical infrastructure,whoeveroperatesit,canwithstandforeigninterference or disruption. The co-rapporteurshavethereforetakenaproportionateapproach,limitedtoa small number of criticalsectors,whichgenuinelystrengthenstheirresiliencewhilekeeping costs and bureaucracy toaminimum,buildingonwhattheseoperatorsalreadydounder existing Union rules. UnderArticle31,assessmentsareintegratedintoexistingNIS2orDORA risk-management frameworks, with no duplicate assessments, audits or reporting. Requirements concern onlycloudservicesandworkloadsthatmateriallyanddirectlysupport an identified critical activity,ratherthanthecompanyasawhole.Transitionalarrangements and a derogation wheresuitablyrecognisedservicesareunavailableonreasonableterms support continuity andpracticalimplementation.

Finally, the frameworkmustremainopentotrustedpartnerswithoutbecomingaloophole. Opening the highestlevelstoprovidersfromthirdcountriesshouldthereforebenarrowand legally certain: thehighestassurancelevelshouldremainreservedforprovidersunder European control,recognitionoftrustedpartnersshouldbelimitedtoLevel3andbasedon clear and verifiablecriteria,andnoownershipstructureorcontractualarrangementshould allow a providerunderforeigncontroltoqualifyindirectly.TheLevel3routefortrusted partners combinescooperationwithverifiablelegal,technicalandorganisationalsafeguards against foreigninterferenceandservicedisruption.

Conclusion

The co-rapporteurssharetheconvictionthatEuropemustreduceitsdependenceonahandful of foreignprovidersandregainthecapacitytobuildthetechnologiesonwhichitseconomy, its securityanditsdemocracyincreasinglydepend.ThatrequiresEuropeancompaniesableto grow, scaleandcompete,startingintheirhomemarket.Thedraftreportreflectsthatcommon ground: fastercapacitybuildingthatrespectshighenvironmentalstandardsandthatlocal communitiescansupport,andasovereigntyframeworkthatisdemandingwhereitmatters, harmonisedacrosstheUnionandworkableforthosewhomustapplyit.Thedraftcombines support forEuropeanproviderswithopennesstointernationalinvestment,fasterdeployment and safeguardsproportionatetothesensitivityoftheactivityconcerned.Theco-rapporteurs look forwardtoconstructivecooperationwiththeshadowrapporteurs,theCouncilandthe Commissiontodelivera Regulationthatmatchesthe scale of thechallenge.

Democrata

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)

Demócrata

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

(Text with EEA relevance)

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 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.

---

[1] OJC ,,p. .

[2] OJC ,,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) 165final.

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

[5] Regulation(EU)2023/2854oftheEuropeanParliamentandoftheCouncilof13 December2023onharmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828(DataAct)(OJL 2023/2854,22.12.2023,ELI:http://data.europa.eu/eli/reg/2023/2854/oj).

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

(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'). The

(4) 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.

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

(7) 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

(8) 173(3)oftheTreatyontheFunctioningoftheEuropeanUnion(TFEU).Such measures should not entail the harmonisation of national laws or regulations. To that

[7] AsdefinedinTitleI,Article2,oftheAnnextoCommissionRecommendation2003/361/ECof6 May2003 concerningthedefinitionofmicro,smallandmedium-sizedenterprises(OJL 124,20.5.2003,p. 36,ELI: http://data.europa.eu/eli/reco/2003/361/oj).

[8] Asdefinedinpoint2oftheAnnextoCommissionRecommendation(EU)2025/1099of21 May2025onthe 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'), September2024,https://data.europa.eu/doi/10.2872/9356120.

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

[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 .

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) 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

[12] Directive(EU) 2022/2555oftheEuropeanParliamentandoftheCouncilof14 December2022onmeasuresfora highcommonlevelofcybersecurityacrosstheUnion,amendingRegulation(EU)No 910/2014and Directive(EU) 2018/1972,andrepealingDirective(EU) 2016/1148(NIS2Directive)(OJ L 333, 27.12.2022,p. 80,ELI:http://data.europa.eu/eli/dir/2022/2555/oj).

[13] Regulation(EU)2024/1689oftheEuropeanParliamentandoftheCouncilof13 June2024layingdown harmonisedrulesonartificialintelligenceandamendingRegulations(EC)No 300/2008,(EU) No 167/2013,(EU)No 168/2013,(EU)2018/858,(EU)2018/1139and(EU)2019/2144andDirectives 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).

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 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.

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

(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

Domoara

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 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

[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)No912/2010,(EU)No1285/2013and(EU)No377/2014andDecisionNo541/2014/EU(OJL 170, 12.5.2021,p. 69,ELI:http://data.europa.eu/eli/reg/2021/696/oj).

[16] Decision(EU)2022/2481oftheEuropeanParliamentandoftheCouncilof14 December2022establishingthe Digital Decade Policy Programme 2030, (OJ L 323, 19.12.2022, p. 4, ELI: http://data.europa.eu/eli/dec/2022/2481/oj).

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) TheCloudandAILeadershipInitiativesshouldalsoensuretheuptakeofcloud 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.

(24a) As AI models and systems are increasingly used in sensitive contexts, public authorities, businesses and citizens need to be able to verify claims made about them, such as how and where a model was developed, which model produced a given output or whether a system has the security properties announced, without necessarily accessing protected information. The Cloud and AI Leadership Initiatives should therefore support the development, testing and deployment of verification technologies, including through dedicated test beds, confidential computing and European standards, so that trust in AI systems can rest on evidence rather than on self-declaration.

(25) MemberStatesshouldestablishExperienceandaccelerationcentresforAI('Centresfor 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,

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.

17

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 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

[18] CouncilRegulation(EU)2021/2085of19 November2021establishingtheJointUndertakingsunderHorizon Europeandrepealing Regulations(EC)No 219/2007,(EU)No 557/2014,(EU)No 558/2014,(EU) No 559/2014,(EU)No 560/2014,(EU)No 561/2014and(EU)No 642/2014(OJL 427,30.11.2021, p. 17,ELI:http://data.europa.eu/eli/reg/2021/2085/oj).

[19] CouncilRegulation(EU)2021/1173of13 July2021onestablishingtheEuropeanHighPerformanceComputing JointUndertakingandrepealingRegulation(EU)2018/1488(OJL 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).

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

(30) TheCommissionshouldreceiveadvicefromstakeholderswithappropriateexpertiseon 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.Suchcoordinationshouldaimtomaximisetheimpactof publicinvestments, avoid duplication of funding, promote alignment of priorities across governance levels, and facilitatethescaling-upanddeploymentofresultsacrosstheUnion.

(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 notab~~ly include the 'AI first' principle defined in the Apply AI Strategy, ur~~ging ***encourage*** organisations to reflect on their business processes, considering the ne~~eds of~~ an ***and the*** 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, 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. ***Given the scale of public support they receive and the strategic nature of the models they develop, entities undertaking such projects should also commit to the safety obligations laid down for general-purpose AI models with systemic risk, irrespective of the classification of their models.***

(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

[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).

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) Datacentresarecriticalinfrastructurefortheunion,andcancreatesubstantial 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, ***Member States should be able to designate*** acceleration zo~~nes should be designat~~edwhere 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 ***carry out an impact*** analysis for each ***before designating an*** acceleration zone, identifying its current and future ***. Carrying out that analysis once, at the level of the zone, reduces the need for developers to repeat, for each data centre project, assessments already made for the zone, and ensures that only sites genuinely suitable for data centre development are designated. In particular, each zone should be supported by firm grid capacity confirmed by the relevant system operators, and its projected electricity demand should be compatible with the national*** energy ***and climate plan, the decarbonisation of the electricity system and the*** needs ***of households and other sectors, including as regards electricity prices***. 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.

(38a) The Union's data centre expansion can only succeed if it is supported by the communities that host it. Data centres use local land, energy and water, and those communities should share fully in the value they create. Projects that deliver tangible and lasting local benefits gain public acceptance, face fewer legal challenges and can therefore be deployed faster and with greater investment certainty. Member States should therefore ensure that every data centre project deployed in an acceleration zone benefits the local communities concerned, in particular through mutual benefit agreements between operators and local authorities, such as the reuse of waste heat for households and public buildings, local employment and training, contributions to local funds or infrastructure, and access to computing capacity for local public bodies, research institutions and SMEs. That expectation should apply equally to all operators, irrespective of their nationality or place of establishment, without constituting disproportionate preconditions for the designation of acceleration zones.

(39) When setting ***minimum*** sustainability requirements for data centres deployed in data centre acceleration zones***, including on energy efficiency, water use and the share of renewable energy***, 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***. Complementary information on on-site and back-up generation, cooling substances and water discharge should allow competent authorities to monitor the local environmental footprint of data centres, without duplicating reporting already required under that Directive***. 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 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. _____

(39a) Acceleration zones are the result of significant public effort: Member States plan the sites, secure grid capacity, carry out the impact analysis and simplify procedures. The Union should ensure that part of the benefits of that effort accrues to genuine

[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).

European businesses, whose growth is essential to closing the Union's capacity gap, keeping investment, jobs and know-how in the Union and strengthening the resilience of its digital infrastructure. European operators often do not have the same financial resources as large competitors from third countries, which can secure land and grid capacity faster and at greater scale. Operators established in the Union and not controlled from third countries should therefore have limited prior access in each zone, giving them the time needed to mobilise investment without being overtaken. In larger zones, a share of available land and grid capacity should also remain reserved for them for a limited period, so that they keep a meaningful place even where they cannot commit within the initial window. So as not to slow down the deployment of capacity, that prior access should be limited in time and lapse without timely follow-up, and all remaining capacity should stay open to every operator on fair, reasonable and non-discriminatory terms. For the same reasons, European businesses, including SMEs and start-ups, should have prior access to newly available colocation capacity in those zones.

(39b) In addition to the facilitation provided within acceleration zones, Member States should be able to offer further incentives for the development of secure and resilient data centre and cloud capacity in those zones, such as support for permitting, infrastructure readiness, skills or investment partnerships. Such incentives should be transparent, objective and non-discriminatory, comply with Union law, including State aid rules, and preserve effective competition.

(39c) Public access to information on the energy, water and environmental impact of data centre projects is essential for local communities, for public scrutiny and for trust in the acceleration zones. The additional information that data centre operators must make available to the competent authorities under Article 11(1), point (a), covers on-site energy generation, emissions, the use of chemicals and refrigerants, and water sourcing and discharge. It should be made available to the public through the register kept by the single information point under Article 12, in a form that allows citizens to understand the impact of each project on the area concerned. The aim is to give the public as much information as possible. The register should therefore be limited only where sectoral Union law, such as Directive (EU) 2023/1791, expressly restricts the disclosure of specific information. The term "aggregated" in Article 12 refers to how information is presented, for example by bringing together the data on a project in a clear and accessible format, and should not be understood as a means of withholding information from the public. An aggregated version should contain all relevant information on the project, and any information left out should be limited to what such an express legal restriction requires.

(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]). ***Member States with decentralised structures should be able to organise those points at regional level, provided that each project keeps a single contact point. Single information points should also serve the public and municipalities, as transparency on projects and their impacts, and the***

[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).

possibility to raise concerns, support the local acceptance on which rapid deployment depends.

(41) Regulation (EU) 202X/XXX [on speeding-up environmental assessments] ([27]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 and accommodating the need for accelerated deployment in certain strategic sectors, while 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. _____ ***That permit should build on the impact analysis carried out for the zone, so that assessments are prepared once by the public authorities rather than repeated by each developer. To make the time limit for individual projects, including the extension or modernisation of existing data centres, effective and predictable, the authorisations required should be processed in parallel, the time limit should start only once the application is complete, and requests for additional information or extensions should be reasoned and limited to what is strictly necessary, in full respect of environmental assessment, public participation and access to justice. Since renewable generation and storage located on site or nearby can supply data centres while grid connections are pending and relieve pressure on the grid, the permits for such facilities should follow the same procedure and time limit.***

(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***. As strategic status confers significant advantages, it should be reserved for projects that combine several contributions. Since strategic projects are intended to reduce the Union's dependencies, the Commission should also be able to take into account third-country control over a project, on the basis of verifiable evidence on ownership and decision-making powers rather than the nationality of individuals***. Considering the importance of the data centre strategic projects, Member

[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.

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 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 ***priority access to*** 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***, without any automatic entitlement to funding***. 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.

(43a) Member States may, in the exercise of their own competences and subject to Union law, consider investment or tax incentives for genuinely additional economic activity, research and development and capability-building in the Union. Any such measures should be transparent, time-limited and based on objective economic substance and Union value creation, irrespective of the undertaking's ownership or place of incorporation. This Regulation does not harmonise national taxation or prejudge State aid compatibility.

Demócrata

(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***. As capacity figures alone do not show how well that capacity serves the Union, the monitoring should also cover its use and geographical distribution, the environmental and grid impacts of data centres and the strategic dependencies of the Union's cloud and AI ecosystem, so that public support and accelerated procedures can be assessed on the basis of reliable evidence. To avoid additional burden, the Commission should rely on data already available under Union law and publish its findings in an aggregated form that protects commercially sensitive information***. 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.

44a. Computing capacity in the Union is spread across many data centres, many of them individually too small for the most demanding AI workloads. Technological developments increasingly allow capacity located at different sites, including in different Member States, to be used jointly, in particular to train a single AI model across several sites that operate in

[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.

parallel and periodically synchronise their work. Such joint use may allow the Union to make better use of its computing capacity and complement large-scale facilities such as AI gigafactories. It may also ease constraints on the electricity grid, since smaller sites can generally be connected more quickly and can reduce their consumption at peak times without interrupting the training. It may also spread the benefits of data centre deployment more evenly across the Union. Its feasibility depends in particular on available grid capacity and on high-capacity network links between data centres, including across borders. As those technologies are still evolving, the Commission should, in cooperation with the Member States, assess the opportunities they offer, make that assessment public with due regard to public security and, where appropriate, recommend measures to the Member States.

(45) ThisRegulationshouldapplytoUnioninstitutions,bodies,officesandagencies('Union entities') when carrying out procedures for the procurement of cloud computing services and AI systems falling within the scope of this Regulation.

(46) TheUnionstillremainscriticallydependentonalimitednumberofcloudcomputing 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. ExistingUnionlawaddressescybersecurity,dataprotection,interoperabilityanddata portability requirements which cloud computing services are subject to. However, there is

(47) 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. Cloudcomputingserviceprovidershavelaunchedtailoredversionsoftheirservice 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-

(48) 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. Againstthisbackground,thesignificantincreaseinpublicorderconcerns–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

(49)

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').

(51a) The Union cloud computing sovereignty framework should apply to cloud computing service providers that wish to provide their services to Union entities and public sector bodies. It should give those entities and bodies, and the providers themselves, a harmonised and transparent basis on which to rely. The four Union assurance levels, the criteria for each level set out in Annex II and the evidence set out in Annex III reflect essential choices on how the Union addresses its critical dependencies on cloud computing service providers subject to the control of third countries or legal entities established in third countries. Those choices determine the degree of protection against the risks described in the preceding recitals, and they are therefore essential elements of the framework that, in accordance with Article 290 of the Treaty on the Functioning of the European Union, are reserved to the legislator. The Commission should accordingly be empowered to adopt delegated acts to amend Annexes II and III only in order to keep them up to date. It should not be able to alter the four-level architecture, the essential requirements or the categories of addressees established by this Regulation. In particular, it should not remove a criterion or an item of evidence, narrow its scope or extend the possibilities of derogation from it. Any amendment having such an effect should be made only by the European Parliament and the Council, on a proposal from the Commission. This distinction gives cloud computing service providers that invest in meeting a given level, and the Union entities and public sector bodies that rely on it, predictability and legal certainty. To ensure that Annexes II and III remain up to date with new legal and technical developments, the Commission should review them at least every 18 months and submit the findings of that review to the European Parliament and the Council, so that the legislator is informed and can decide on any amendment that falls outside the scope of the

[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).

delegated powers.

(51b) The recognition of a cloud computing service provider at a Union assurance level by one Member State has effect throughout the Union. Cloud computing service providers, public sector bodies and Union entities that rely on a recognition in one Member State therefore need to be able to trust that the criteria for recognition are applied in the same way in every Member State. Divergent application of those criteria would undermine that trust, would distort competition between providers according to the Member State in which they apply, would encourage providers to seek recognition where the criteria are applied least strictly, and would fragment the internal market that the Union assurance levels are meant to support. It is therefore necessary to provide for a common methodology, for monitoring and annual reporting by the Commission, and for a procedure enabling the Commission to act where a Member State systematically does not apply the criteria uniformly. In that procedure, the Commission may take into account reasoned objections raised by competent authorities in the course of recognition procedures. That procedure should be graduated and proportionate. The Commission should first hear the Member State concerned and, where it considers that action is needed, issue a reasoned warning that identifies the specific shortcomings, the measures to be taken and a clear timeline for taking them. That timeline should in principle be no shorter than the minimum period set out in this Regulation, so that the Member State has a real opportunity to correct its enforcement, and it may be shorter only where the situation requires urgent action. A suspension of the ability of a Member State's competent authorities to recognise providers should be possible only where the Member State has not taken those measures within that timeline. A clear and predictable timeline gives the Member State the opportunity to correct its enforcement and gives businesses legal certainty on whether, when and under what conditions recognition decisions may be affected, so that they can plan their investments and their dealings with public sector customers. Any suspension should be temporary and lifted as soon as uniform application is ensured. Throughout the procedure, the Commission and the Member State concerned should coordinate in order to implement the necessary measures swiftly. The possibility for the Commission to take over recognition temporarily should be possible only where a suspension has not led to the necessary corrective measures, and should be subject to the conditions set out in this Regulation for the Commission acting as evaluating authority.

(52) TheUnionassurancelevelsshouldprovideforaproportionateframeworktoensurethat 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.

(52a) The assessment of Union assurance levels should focus on effective legal and operational control, verified resilience and the ability to protect customer data and maintain the audited service when external technology suppliers are unavailable. Reliance on global software and hardware supply chains should not, as such, disqualify a service, provided that all criteria applicable to the requested Union

assurance level, including any requirements on third-country control, continue to be met.

(52b) The recognition of a cloud computing service provider at a Union assurance level should follow a clear and harmonised procedure. A provider should apply to the competent authority of the Member State in which it has its main establishment. That authority acts as evaluating authority and assesses the application on the basis of the evidence required for the requested level. For level 1, that is the EU statement of conformity, and for levels 2 to 4, the audit report, the positive audit opinion and the supporting evidence. To limit the burden on applicants, in particular SMEs, evidence that is already available through recognised Union certifications or registers, and that is relevant, current and sufficient, should not be requested again, and the EU statement of conformity of an SME at level 1 should be recognised directly in all Member States. The application should identify the service concerned and its critical subcontractors, together with their functions, access rights and dependencies, so that the evaluating authority can verify the criteria on the basis of the actual structure of the service. Recognition should be determined by the criteria applicable to the audited service and the requested level. The nationality of a shareholder should not, of itself, justify a refusal where it confers no effective control, privileged access or other relevant legal exposure. This does not affect the ownership and control requirements that Annex II expressly sets out. Because a recognition has effect throughout the Union, the competent authorities of the other Member States and the Commission should have the opportunity to review each draft recognition decision and, where they consider that it does not comply with the applicable level or with the methodology for uniform application, to submit a reasoned objection or a request for clarification. The evaluating authority should take due account of them. Where it maintains its draft decision, the matter should be capable of being referred to the Commission, which should be able to take a binding decision, or in accordance with Article 16a, take over enforcement temporarily. Fixed time limits for each step, including an acknowledgement that the application is complete, should give applicants predictability on when they can expect a decision. The evaluating authority should give the applicant the opportunity to comment before it rejects an application. Recognition should be suspended where a provider has intentionally or negligently supplied incorrect or misleading information, and the other Member States and, where applicable, the Commission should be informed without delay.

(52c) The personnel requirements in Annex II are intended to address the risks that arise from persons who can actually influence the security, continuity or sovereign operation of the audited service. They should therefore apply to persons who are directly involved in the provision or administration of the service, or who exercise privileged operational control over it, including through logical or physical access to customer data, to the management or control plane, or to the hardware or software stack used to provide the service. This applies whether those persons are employed by the cloud computing service provider or by a subcontractor. The requirements should not extend to the provider's workforce as a whole, or to staff whose functions have no connection to the audited service and who have no such access or control, such as personnel working in human resources, marketing, sales or general administration, or on other services of the provider that are unrelated to the audited service. This clarification is meant to keep the requirements proportionate, so that they are not applied to persons who cannot affect the audited service, and it avoids unnecessary

Document

burdens, in particular for providers that offer several services or that are SMEs. It does not create an exemption: whether a person is covered should depend on the function actually performed and on the access or control the person has or is capable of exercising, and not on the person's job title, the department in which the person works, or how the provider has organised its workforce.

(52c) Evaluating applications for recognition should remain, as a rule, a task of the competent authority of the Member State of main establishment. At the same time, a provider that operates in several Member States should not need to deal with divergent procedures. The Commission should therefore be able to act as evaluating authority for applications from such providers, but only where the Member State of main establishment has expressly conferred that task on it and the provider has chosen to apply to the Commission. A Member State should be free to define the scope of the conferral, including the assurance levels it covers, and to withdraw it with appropriate notice. Applications pending at the time of withdrawal should be completed by the Commission so that applicants are not left without a decision. The Commission should also be able to act as evaluating authority where, as a last resort under the procedure for the uniform application of the criteria, it temporarily takes over recognition because a Member State has not taken the corrective measures required. That take-over should end as soon as the Commission has established that the Member State ensures uniform application. Where the Commission acts as evaluating authority, the procedural guarantees applicable to national authorities should apply in the same way, so that the competent authorities of the Member States can submit reasoned objections and requests for clarification. As the Commission cannot be the arbiter of its own draft decision, the mechanism for referring disputes to the Commission should not apply. Instead, the Commission should consult the authorities that submitted objections before it takes its final decision. The competent authority of the Member State of main establishment should assist the Commission and provide the relevant information without undue delay.

(52d) Some cloud computing service providers are subject to the control of a third country with which the Union has close ties and a high degree of legal and regulatory convergence. It is appropriate to provide a narrow mechanism under which the Commission can identify such associated third countries, so that providers subject to their control may be audited against the criteria for Union assurance level 3, but not level 4. Third-country arrangements should not dilute the most demanding sovereignty guarantees. Any eligibility decision should rely on a transparent assessment of the third-country legal environment, enforceability of safeguards, independent audit and continuity arrangements. A narrow, reviewable mechanism can support trusted international technology supply chains to support Union sovereignty endeavours while ensuring that strategic public-sector uses remain subject to the Union requirements applicable to their level. A third country should be identified only where it fulfils the cumulative criteria set out in this Regulation, and the Commission should repeal, amend or suspend its decision where it no longer does so. A transitional period should be an exception. It should be granted only where strictly necessary to ensure the continuity of essential services, should be reasoned and time-limited, and should be extended once at most, on the basis of a documented migration plan. It should not be granted where an immediate serious security risk requires suspension, and it should not serve to maintain or reinforce the market

position of any provider. The Commission should publish a list of the third countries that fulfil the criteria and those that no longer do so, to give legal certainty to providers, public sector bodies and Union entities.

(53) Itisimportantthatnationalcompetentauthoritiesofestablishmentofthecloud 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 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. ***The self-assessment should be service-specific and supported by a standardised declaration and evidence proportionate to Union assurance level.***

(55) Independent audits are an important tool for monitoring the compliance of cloud compuring ***computing*** services providedby cloud computing service ***providers***. Given the need to ensure that the applicable criteria for Union assurance levels 2, 3 or 4 are verified by third-party independent experts, cloud computing service providers should be accountable, through independent auditing, for their compliance with the criteria set out by this Regulation. Cloud computing service providers should be free to select the auditing organisation ***CADA auditor or audit firm*** of their choice as long as the auditing organisation ***it has been approved by the competent authority of a Member State and*** demonstrates the necessary independence and compliance with the requirements in this Regulation***. Audits should be carried out at the provider's own expense and should be limited to the service and controls relevant to the assurance level sought***. 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 ***them*** access to all relevant data and premises necessary to perform the audit properly and answering oral or written questions. Auditing organisations ***CADA auditor or audit firm*** 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 ***and CADA auditors and audit firms should maintain professional scepticism throughout the audit. CADA auditor or audit firm*** 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

Democratia

audit obligations in this Regulation. A~~uditing organisations~~ ***CADA auditor or audit firms*** should have the necessary expertise in risk management and technical competence to audit cloud computing services. They ***Member States should approve only those that are of good repute, have proven expertise, objectivity and professional ethics, and should enter them in a public register. Member States may treat statutory auditors and audit firms approved under Directive 2006/43/EC as approved under this Regulation where they also have the required expertise. CADA auditor or audit firms*** should comply with core independence requirements for prohibited non-auditing services, firm rotation ***a cooling-off period for previous audit engagements*** and non-contingent fees***. Independence should be assessed on the basis of documented checks of actual and potential conflicts of interest, the effective separation of incompatible services and appropriate rotation or independent review arrangements, proportionate to the risk and duration of the engagement***. If their independence or technical competence of auditing organisationsis not beyond doubt, they should abstain or resign from the audit engagement.

(55a) The assessment of the compliance of the audited service with the criteria set out in Annex II should rely on the audit evidence listed in Annex III. That evidence should be relevant, sufficient, reliable, necessary and proportionate to the requested Union assurance level. Independent auditing is essential for the higher levels, but repeating evidence already examined under a relevant and equivalent certification, or already independently verified under applicable Union law, adds cost without automatically improving assurance. Reuse of such evidence should be conditional on the same service boundary, current validity, a competent auditor and full coverage of the sovereignty criterion at issue. To give legal certainty on reuse, the Commission should recognise certification schemes, such as those under the Union cybersecurity certification framework, whose requirements are equivalent to or more stringent than one or more criteria of Annex II. Only schemes established or overseen by a public authority of the Union or of a Member State, that require independent third-party audit and periodic re-audit and provide for suspension and withdrawal of certificates, should be recognised. A valid certificate issued under a recognised scheme should be accepted as evidence of compliance with the criteria it is recognised as demonstrating, while the CADA auditor or audit firm should verify its validity and scope and assess the remaining criteria. Recognition of a scheme should not in itself establish conformity with an ownership, foreign-law exposure, jurisdictional control or operational-autonomy criterion, unless that precise criterion falls within the independently verified scope of the scheme. Obligations under Directive (EU) 2022/2555 (NIS2) and Regulation (EU) 2022/2554 (DORA) may likewise provide useful evidence, but neither certification nor those obligations should be treated as automatic proof of sovereignty. Where a subcontractor involved in the provision of the audited service operates a cloud computing service that is registered in the central repository as recognised at the same or a higher Union assurance level, that recognition should be accepted as sufficient evidence for the criteria it already covers, without the audited provider having to reproduce that evidence. The audited provider should remain responsible for the criteria applying to its own layer of the service. For specialised cybersecurity functions, alternative technical controls may be accepted where equivalent assurance is demonstrated and they demonstrably preserve the required sovereignty outcome, ensure incident response and do not permit uncontrolled access to protected data. Mandatory disclosure of proprietary third-party source code may be legally impossible for

European cloud providers that rely on licensed software, and could unintentionally exclude them from the market. Independent testing, attestations, reproducible security evidence and contractual controls may provide an equivalent assurance outcome, subject to scrutiny by the CADA auditor or audit firm. That alternative is not an unconditional waiver: it should be rejected wherever the specific risk cannot be adequately evidenced or mitigated or the source code could reasonably have been obtained.

(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 ***declaration of interests, a list of the third parties consulted and*** 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***, and the report should then state the Union assurance level to be recognised***. A 'negative opinion' should be given where the auditing organisations ***CADA auditor or audit firm*** considers that the provider does not comply with the criteria set out in this Regulation***, and should be accompanied by operational recommendations on the measures needed to achieve compliance and the recommended timeframe***. 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. ***To keep a recognition up to date, the audited provider should submit the audit report and the positive opinion each year to the same or a different CADA auditor or audit firm for review. That review should focus on material changes and critical controls, and a full reassessment should be required only where those changes materially affect the recognised level or where justified by risk. On that basis, the CADA auditor or audit firm may confirm, update or revoke the report and opinion, and may also revoke them where the provider has intentionally or negligently supplied incorrect or misleading audit evidence. The Commission should be empowered to adopt delegated acts on the performance of audits, including procedural steps, rules for CADA auditors and audit firms, auditing methodologies and templates for audit reports.***

(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 ***~~CADA auditor or audit firm~~***, competent authorities and the Commission. ***The repository should be publicly available and machine-readable, specify the scope, validity and assurance level of each recognised service, and be kept up to date, including as regards revocations, without disclosing protected security-sensitive information.***

(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

Document

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 *cloud computing services*~~ and the supervision of recognised cloud computing service providers ***without prejudice to the role of the Commission as evaluating authority where this Regulation so provides***. 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***. To that end, their members should remain free from external influence and should not seek or take instructions from anybody, and each authority should have its own staff, subject to its exclusive direction, and separate, public annual budgets, while remaining subject to financial control that does not affect its independence. Where the Commission acts as evaluating authority, it should have corresponding investigative powers, exercising inspections of premises in a Member State through the national competent authority of that Member State, and, where a Member State has conferred that task on it, the enforcement powers of the national authority, which should then no longer exercise them in respect of the providers concerned. The Commission should also be subject to equivalent requirements of impartiality, transparency and independence from cloud computing service providers, with the necessary adaptations***. 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. ***The authority of the Member State of main establishment of a provider should have exclusive competence for enforcing this Chapter and should act as the coordinating contact point for cross-border supervision, without prejudice to the powers of other competent authorities and of the Commission.*** 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 ***and the Commission*** 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 ***and with the Commission*** 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) TheUnion'sobjectiveofstrengtheningitsautonomyshouldbepursuedinamannerthat 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 ***or*** in the areas of national security, internal security, external ~~bor~~der 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.

Democrata

(62a) In order to ensure legal clarity and predictability, and to prevent the fragmentation of the internal market that divergent national risk assessments would otherwise cause, Annex IIa sets out, for each Union assurance level, a non-exhaustive list of public sector activities to which that level applies. As a matter of principle, each listed activity should thereby receive the same level of protection throughout the Union, providing a harmonised framework for cloud computing service providers and public authorities alike. The Union assurance level of activities not listed in Annex IIa should continue to be determined by the risk assessments of Member States and Union entities. Since the listed activities are identified by the data and services concerned, the applicable level should not depend on the administrative level or legal form of the public sector body or Union entity carrying them out, or on whether a Member State has chosen to apply Directive (EU) 2022/2555 to that body. Some of the most sensitive data held by public authorities, such as population and civil-status registers, health records, and social security and tax records, are held by bodies that do not necessarily fall within the sectors covered by that Directive or the areas of security, defence, justice and border management, such as local authorities and bodies governed by public law, including statutory health insurers. Annex IIa does not, however, extend this Regulation to entities other than public sector bodies and Union entities. In duly justified cases, Member States and Union entities should nevertheless be able to assign a different Union assurance level to a specific activity listed in Annex IIa, on the basis of a documented risk assessment notified to the Commission.

(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 ***complementing Annex IIa,*** 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.

Democrata

(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***, or which carry out activities listed in Annex IIa,*** should therefore procure

only the cloud computing service ~~providing the appropriate level of~~ ***recognised at least at the Union*** assurance betwe~~en levels 2 and 4~~ ***level d*****etermined for the activity concerned**. 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.

(64a) The Union assurance level required for an activity should apply to the cloud computing service actually used to perform the contract, including where that service is supplied through a reseller, integrator or managed service provider, so that the level cannot be met merely through the identity of the contracting partner. For the same reason, where a recognised service ceases to offer the required Union assurance level following a change of control, the contracting authority should be able to terminate the contract without penalty. That right should be triggered by the loss of the required level and not by the change of control as such.

(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~~ ***Certain*** ~~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~~ ***that are not public sector bodies but operate in*** sectors ***of high criticality listed*** in Annex I to Directive (EU) 2022/2555 to be able tocarry out the same assessments as ***activities on which the functioning of society and the economy depends. For a limited number of activities or data, the disruption of, or unauthorised access to, the cloud computing services they rely on could have effects comparable to*** those carried out by ***affecting public sector bodies, endangering public order in the*** Union***. It is therefore necessary and proportionate that those*** entities and Member States ***assess whether any of their activities require Union assurance levels, 2, 3 or 4. To avoid unnecessary burden, that assessment should form part of the cybersecurity risk-management measures they already take under that Directive or, for financial entities, under Regulation (EU) 2022/2554, and should not be a separate procedure. The applicability of a Union assurance requirement should be determined by reference to the particular critical service, operation or workload and should not automatically extend to all activities or cloud environments of the entity concerned. Where critical and non-critical activities rely on shared infrastructure, effective segregation may demonstrate compliance without requiring the entire environment to be subject to the same Union assurance level. Where the assessment concludes that Union assurance level 2, 3 or 4 is not critically necessary, those entities should remain free to choose any cloud computing service, without being required to use services recognised at Union assurance level 1.***

Delegata

(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 ***of objectively verifiable contributions, irrespective of the tenderer's place of incorporation, such as*** helping reinforce the digital supply chain in the Union; integrating Union technologies; conducting the innovation required to deliver the service in the Union; and delivering the service using hardware components designed or manufactured in the Union. ***Union or, where such components are not reasonably available, equivalent auditable contributions to resilience and secure supply; ensuring operational autonomy and continuity of the service; contributing to the maintenance of open source components; and enabling migration to another provider.*** 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 ***At*** this ***the*** purpose, ***same*** contracting ***time,*** authorities ***in*** could ***order*** consider a maximum weighting of 15 out of 120 points to be allocated to ***for*** European added value within ***to have a meaningful effect on*** the overall ***award,*** evaluation ***the*** methodology***. criteria*** ensuring ***relating*** that ***to*** it remains ***should together account for at least 20 % of the total weighting of the award criteria, the weighting of each subcriterion being*** proportionate and ***to*** subordinate ***its relevance*** to the core ***subject-matter*** contract ***of*** award ***the*** criteria. ***contract.***

(67a) Higher Union assurance levels can offer greater protection against risks to the security, resilience and continuity of cloud computing services, including unlawful access and supply disruption. Contracting authorities should therefore have the possibility, but not the obligation, to reward such additional protection through a non-price award criterion, without prejudice to the minimum assurance levels required under this Regulation. In order to ensure equal treatment and proportionality, that criterion should be transparent, reflect the security benefit for the intended use, be subject to a maximum weighting and be applied in accordance with Union public procurement law. Since the Union assurance level is a characteristic of the service offered, it should be considered to be linked to the subject-matter of the contract.

(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% ***35%*** 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. Inthejointdeclarations'Buildingthenext-generationcloudforbusinessesandthe 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

(69)

Joint declaration, 'Building the next generation cloud for businesses and the public sector in the EU', 15.10.2020,

30 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 .

working towards the deployment of a secure and interoperable European public-sector cloudfederation.InitsconclusionsonthefutureofEUdigitalpolicyof21 May2024 (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. 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.

(71)

(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

[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.

[33] Regulation(EU)2024/2847oftheEuropeanParliamentandoftheCouncilof23 October2024onhorizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013and(EU)2019/1020andDirective(EU)2020/1828(CyberResilienceAct)(OJL, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

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 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.

[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).

(76) TheCommissionshouldpresenttotheMemberStatesadraftagreementsettingoutthe 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 ~~procedure~~ ***procedure. That presumption should not affect the obligation to use cloud computing services recognised at the Union assurance level required under this Regulation, including where software or AI systems are delivered through such services***.

(78) Theagreementshouldestablishasteeringcommitteecomposedofthe Commissionand 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.

(78a) Under framework agreements, contracting authorities are not obliged to purchase, and orders often fall well short of the maximum value announced. That uncertainty makes it difficult for providers, in particular SMEs and start-ups, to rely on such agreements when seeking financing. A committed public contract can instead serve as an anchor that allows them to obtain the financing they need to invest in capacity, while giving public buyers a stronger supply of recognised services at competitive prices. Participating entities should therefore be able, on a voluntary basis, to commit to purchasing a guaranteed minimum share of the estimated value of a procurement for activities assigned Union assurance level 3 or 4.

(79) Therulesgoverningresponsibilityandtheapplicablepublicprocurementframework 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

Demócrata

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) Inordertoensurethatthenecessaryresourcesremainavailable,theparticipatingentities 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) Opensourceplaysanimportantroleinensuringtransparency,securityandefficiencyin 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

Democrata

(82) To ensure the efficient, transparent and interoperable use of digital technologies across the Union's public sector, it is necessary for ***Union entities and*** public admini~~strations to promo~~te ***sector ~~bodies to~~ give preference, where technically feasible and relevant, to*** open standards and components released under an open source licence when building their cloud and AI ecosystem or stack.

(82a) The promotion of open standards and of components and solutions released under an open source licence is intended to ensure that Union entities and public sector bodies give them genuine consideration when defining their needs and when procuring or developing cloud and AI solutions. It is not intended to oblige them to switch to open source solutions, to replace solutions that they already use, or to exclude proprietary solutions. The preference should apply only where an open source solution is technically suitable and meets the needs of the contracting authority. It should therefore be exercised case by case, on the basis of an assessment of functionality, security, service continuity, operational support, exit capability and total cost, including the cost of exiting the solution, and of other relevant, duly justified objective criteria. Where such an assessment shows that an open source solution is not the most suitable one, the contracting authority should be free to choose another solution, provided that its choice is justified. The preference should be exercised in line with the principles of equal treatment, non-discrimination, transparency and proportionality. It may take the form of specifications, award criteria or conditions for the performance of contracts, and it applies irrespective of the value of the contract. The EU OSS Catalogue should serve as a source of information that helps contracting authorities identify suitable open source solutions.

(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 decideto make software ***to which they hold intellectual property rights*** ~~available~~ for reuse to do so ***under an open-source licence*** in a catalogue or repository that is connected to EU Open Source Solutions Catalogue (‘the EU OSS Catalogue’)***. Since that obligation pursues the same objectives of security and autonomy as the promotion of open source, it should not apply where publication would itself undermine those objectives or other interests protected by Union law. In such cases, reuse may still be achieved through secure sharing between public bodies***. 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.

(83a) Many cloud computing services and AI systems provided in the Union depend on open source components that are often maintained by a small number of contributors without stable funding. Where such components are critical, insufficient maintenance or the loss of their maintainers creates security and continuity risks for the whole ecosystem. The Union should therefore identify those components and support their maintenance, security remediation and long-term continuity, in cooperation with open source software stewards. In order to preserve the ability to maintain and, where necessary, independently continue the development of those components, a critical mass of Union-based contributors should be ensured, including for technologies originally developed outside the Union.

(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.

(84a) The personnel requirements laid down in Annex II for Union assurance levels 3 and 4 are intended to address the risks that arise from persons who can actually influence the security, continuity or sovereign operation of the audited service. They should therefore apply to persons who are directly involved in the provision or administration of the service, or who exercise privileged operational control over it, including through logical or physical access to customer data, to the management or control plane, or to the hardware or software stack used to provide the service. This

[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).

applies whether those persons are employed by the cloud computing service provider or by a subcontractor. The requirements should not extend to the provider's workforce as a whole, or to staff whose functions have no connection to the audited service and who have no such access or control, such as personnel working in human resources, marketing, sales or general administration, or on other services of the provider that are unrelated to the audited service. This clarification is meant to keep the requirements proportionate, so that they are not applied to persons who cannot affect the audited service, and it avoids unnecessary burdens, in particular for providers that offer several services or that are SMEs. It is not intended to create an exemption. Whether a person is covered should depend on the function actually performed and on the access or control the person has or is capable of exercising, and not on the person's job title, the department in which the person works, or how the provider has organised its workforce. The same approach should apply to the personnel of subcontractors, as defined in Article 2 of this Regulation.

(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 theprinciplessetoutintheInterinstitutionalAgreementof13 April2016onBetter 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 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

[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).

[37] Regulation(EU)No 182/2011oftheEuropeanParliamentandoftheCouncilof16 February2011layingdown 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).

(89) Article 42(1) of Regulation (EU) 2018/1725 ([38]). 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:

Demócrata

[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;

Demócrata

(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

Demócrata

(25) (1), of Directive 2014/24/EU; ‘opensourcelicence’meansopensourcelicenceasdefinedinArticle2,point(12),of Regulation (EU) 2024/903.

(26) 'subcontractor' means a natural or legal person engaged by a cloud computing service provider to perform functions that contribute to the provision, operation, security or effective control of a cloud computing service within the scope of this Regulation or that has access to or control over components used in or for that service which may affect its security, continuity or sovereign operation. The requirements applicable to that person shall be determined by reference to the functions performed and the control actually exercised or capable of being exercised. The mere supply of ancillary services shall not, in itself, constitute subcontracting. A service is ancillary only where it is not used in or for the provision, operation, security or delivery of the audited service and does not involve logical or physical access to customer data, to the management or control plane or to the hardware or software stack used to provide the service. A person that supplies services used in or for the audited service, shall be presumed to be a subcontractor, unless proven that its service is ancilary. The provider shall document its classification of each subcontractor and make it available to the auditing organisation, which shall verify it.

Demócrata

TITLE II
RESEARCH, DEVELOPMENT AND DEPLOYMENT ACTIVITIES FOR THE CLOUD AND AI ECOSYSTEM
Chapter I
Cloud and AI Leadership Initiatives
Article 3
General objectiveoftheCloudandAILeadershipInitiatives

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 ***energy and*** 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 ***and independence*** of the digital infrastructure***, including through interoperable, portable and multi-provider architectures that reduce avoidable dependencies***;

(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***, through voluntary, demand-driven incentives and competitive access for SMEs and small mid-caps***.

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 ***sovereign*** cloud computing stacks supporting the Union's technological autonomy (operational objective 2);

(c) advancingUnion'scapabilitiesinfrontierAI(operationalobjective3);

(d) advancingUnion'scapabilitiesinphysicalAImodelsandsystemsandfostering their deployment across the Union's strategic sectors (operational objective 4);

(e) acceleratingthedevelopmentanduptakeofindustrialAIacrosstheUnion's strategic sectors (operational objective 5);

(f) supporting the development of advanced platforms for the large-scale deployment of AI agents ***and monitoring their compliance with existing national and EU law*** (operational objective 6);

Democrata

(g) increasingthedevelopmentandadoptionofAImodelsandsystemsacrossthe Union's public sectors (operational objective 7);

(h) increasing the adoption of AI technologies at regional and local level, and the ***competitive*** uptake of cloud computing services provided by European cloud computing service providers***, without excluding other eligible providers solely on grounds of origin, creating verifiable technological and economic value in the Union*** (operational objective 8).

(i) supporting the development and deployment of technologies for the verification of claims about AI development and inference (operational objective 9)

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***, taking into account local water stress, climate conditions and technical and economic feasibility***;

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

(c) developAI-poweredtechnologiesforoptimisingserverefficiency,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 ~~***their flexibility, in coordination with the relevant transmission and distribution system operators and with due regard to grid availability, demand response and security of supply***~~;

(e) leveragedatacentresasanchorclientsforadvancedenergymanagementsystems harnessing diverse energy sources, including small modular reactors and clean hydrogen, alongside efficient energy storage solutions;

(f) deploytestbedsandpilotlinestointegrateandtesttechnologiesdeveloped 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***, based where appropriate on open and documented interfaces, interoperability, portability, verifiable security and multi-provider deployment, without mandating a particular licensing model***;

(b) develop AI-optimised servers and baseline software***, including, where technically feasible and commercially available,*** based ~~onprocess~~ors, accelerators and quantum accelerators designed and manufactured in the Union, alongside next-generation ultra-high density and long-term data storage;

Democrata

(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***, and support the maintenance, security remediation and vulnerability and long-term sustainable governance of the critical open-source components on which the provision of cloud computing services and AI systems in the Union depends***;

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

(f) ***support the development, testing and independent evaluation of security safeguards for openly available AI models, including secure deployment environments, misuse monitoring and methods to assess and mitigate vulnerabilities, without requiring disclosure of protected information or imposing a particular model licence;***

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***, while strengthening reliable access to advanced AI capabilities, operational continuity, independent evaluation and the ability to deploy or adapt models within the Union where lawful and technically feasible***.

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

(c)

(d) develop bilateral initatives with like-minded international partners that lead in the research and development of physical AI technologies in order to foster technological exchange and cooperation, mutual learning and advancement of sovereign physical AI

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

(a) accelerate the development and uptake of se~~ctoral~~ ***specialised sector specific*** 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 enhan~~cing~~ ***ensuring compliance with European rules of data protection and*** privacy and preserving confidentiality***, including federated and distributed processing and verifiable safeguards for personal data, trade secrets and commercially sensitive information***.

Democrata

(c) ensure convergence and cooperation between projects falling under objective 4 (physical AI) and 5, where necessary, in order to advance leadership on industrial AI

6. Under theiroperationalobjective6,theCloudandAILeadershipInitiativesshall:

(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***, including traceable agent actions, secure tool access, human intervention and effectiveincident responseproportionateto theriskof theintendeduse***.

7. Under operationalobjective7 theCloudandAILeadershipInitiatives 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, ***transparency*** and simplify administrative procedures ***while ensuring high quality output***;

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

(d) facilitatesecure,privacy-enhancinghealthdatareuseforAImodelsandtoolsin healthcare;

(e) facilitatethedevelopment,testinganddeploymentofAImodelsandtoolsinthe automotive sector, including for autonomous driving.

8. Under operationalobjective8 theCloudandAILeadershipInitiatives 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')***, with particular attention to first-time adopters, smaller municipalities and less-developed regions, using accessible advisory and demonstration services***;

(b) developacommoncloudandAIcurriculum,drawingonthenetworkofCentres 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) supporttheprocurementofdatacentreservicesandcloudcomputingservicesfor Union entities and public sector bodies.

9. ***Under operational objective 9, the Cloud and AI Leadership Initiatives shall:***

(a) deploy test beds and computing infrastructure dedicated to research on the verification and security of AI models and systems;

(b) support the development and validation of verification technologies, from proof of concept to deployment in operational environments, including through programmes rewarding the disclosure of vulnerabilities, and make the results

Democrata

availableunderanopensourcelicencewheresecurityallows;

(c) accelerate the deployment of technologies, such as confidential computing, that allow AI models and their training data to be evaluated without being disclosed;

(d) contribute to the development of European standards for the verification of AI modelsandsystemswithinthemeaningofRegulation(EU)No1025/2012.

Article 5

Experience and Acceleration Centres for AI

1. Each Member State shall ***designate or*** establish ***one or more*** 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. Theobjectivesof theCentres forAIshallbeto:

(a) supporttheintegrationandscaling-upof AI usecases instrategicindustrialand 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~~ ***where AI is demonstrably suitable, secure and proportionate to needs of the user***;

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

(d) leverage general and dedicated AI infrastructure to accelerate the development of AI verification technologies and safety measures.

3. TheCentres for AI shallbetasked,inparticular,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***, while providing transparent, impartial and provider-neutral advice***;

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

(c) facilitatingthetransfer of expertiseacross regions;

(ca) collaboratingonandexchangingopensourceprojectsofcommoninteresttoUnion entities and public sector bodies;

(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.

(e) assisting SMEs, small mid-caps and start-ups in accessing testing facilities, computing resources, financing opportunities and innovation procurement, including by providing proportionate support for technical documentation,

Democrata

interoperabilitytestingandparticipationincross-borderconsortia;

4. The Commission may adopt implementing ~~acts detailing the procedure for establishing~~ ***specifying only common technical interoperability, minimum transparency and proportionate reporting arrangements for the network of*** Centres for AI***, without prescribing their internal*** ~~and further arrangements concerning participant~~organisation ~~profile, selection criteria and details on the implementation of the~~ ***or substantive*** 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***, including by facilitating interoperable remote access to testing environments and computing capacity under transparent and non-discriminatory conditions***.

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***, without prejudice to the objectives, eligibility conditions, budgetary procedures and governance of those programmes, and without creating an automatic entitlement to Union funding***.

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.

5. The Commission shall publish, at least every two years, a concise assessment of the results of the Cloud and AI Leadership Initiatives, using indicators on private investment mobilised, SME and small mid-cap participation, access to computing resources, interoperability, deployment of European-developed technologies and measurable security and resource-efficiency outcomes. The assessment shall, wherever possible, reuse information already reported under existing Union

programmes and shall not impose additional reporting duties on individual beneficiariesbeyondthoseapplicableundertherelevantfundingprogramme.

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'). ***Member States may fulfil this obligation by updating an existing national digital, cloud or AI strategy, provided that the relevant objectives and measures are clearly identifiable.***

2. Thenationalstrategies shallincludeatleastthefollowing:

(a) objectivesandprioritiesforcloudandAIadoption,inlinewiththe'AIfirst' principle, as well as a governance and monitoring framework to achieve those objectives and priorities;

(b) measurestoacceleratethedevelopmentandadoptionofcloudandAIatnational, 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***, taking into account verified electricity grid capacity, foreseeable power demand, local water availability and consistency with relevant national energy andclimate plansandnetwork developmentplans***;

(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 excellenceandinnovation,includingthrough publicprocurementmeasures,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 enhancethecompetitivenessofstrategicEuropeanindustries;

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

(i) the current and projected data centre and AI compute capacity in the Member States, indicating separaretely the capacity operated by entities subject to control by a third-country or be a legal entity established in a third country.

(j) measures designed to mobilise additional investment in cloud and AI capacity, including research and development, skills, interoperability, energy-efficient

infrastructure and diversification of critical supply chains within the Union, by means of transparent and objectively verifiable support schemes consistent with the Treaties and applicable State aid rules.

3. National strategies shall be consistent with the objectives of this Regulation ***and Regulation 2024/1689.***

4. Member States shall ensure that their national strategies are consistent with, and contributeto,theassociateddigitaltargetsestablished underArticle4ofDecision (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. ***For that purpose, Member States and the Commission shall, wherever possible, reuse information and indicators already reported under Decision (EU) 2022/2481 and other applicable Union instruments and shall not require duplicative reporting on the same measures.***

6. TheEuropeanArtificialIntelligenceBoardestablishedbyRegulation(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.

Demócrata

Article 8

Criteria for frontier AI priority projects

1. The Commission may, by means of a decision, recognise as frontier AI priority projects, projects selected through ***transparent, competitive and publicly announced*** open calls for expression of interest***, with published eligibility and assessment criteria*** 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***, and allows meaningful participation by SMEs, small mid-caps, research organisations and start-ups through transparent consortium arrangements***;

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

(d) it is aimed at reducing technological dependencies to third countries and aimedatbuildinganindependentAIstackacrosstheentirevaluechain

(e) the entities undertaking the project commit to comply, as regards to the AI models developed in the project, with the obligations laid down in Article 55 (1) of Regulatiion (EU) 2024/1689, irrespective of whether those models are classified

as general-purposed AI models with systemic risks.

The Commission shall publish a reasoned decision on recognition, including a summary of the assessment against the criteria in paragraph 1 and the expected Union added value. The decision shall not, by itself, confer a right to funding or computing resources.

Article 9

Computing support for AI projects

1. TheUnionandtheMemberStatesshallensurethatsufficientAIcomputingresources 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 le~~ast ***seek*** ***to*** match the AI computing resources contributed by ***participating*** 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. ***, including specialised, energy-efficient and sector-specific AI models, subject to transparent criteria reflecting expected industrial, scientific and public value, security needs and efficient use of available resources***

4. Access to computing resources supported under this Article shall be organised through transparent, objective and non-discriminatory procedures, with proportionate conditions for SMEs, start-ups, open-source projects and research organisations. Allocation decisions shall respect the governance and access rules of the relevant Union or national infrastructure and shall not require disclosure of commercially sensitive information beyond what is necessary for eligibility and security checks.

Democrata

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 ***may*** des~~ignate~~ at least one ***or ~~more~~*** 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 ***conduct an impact~~-analysis~~ regarding all of*** the following aspects when ***prior to*** designating accelera~~tion z~~ones:

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

(aa) ensure that each designated zone is supported by firm and verified electricity grid capacity, certified by the competent transmission system operator (TSO) or distribution system operator (DSO), together with a binding timetable for grid reinforcement where additional capacity is required;

(b) the available and future power grid capacity and the possibility and conditions for on-site storage and clean energy generation; ***the compatibility of the projected electricity demand of the zone with the integrated National Energy and Climate Plan of the Member State, with the decarbonation of the electricity system and with the electricity needs of households and other sectors, including the expected effect on electricity prices for final consumers;*** the available and future network connectivity capacity;

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

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

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

(f) the preference ***potential*** for reusing brownfield sites over using greenfield sites ***with a preference for location in existing or former heavy industrial areas***;

(g) 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 climat~~e resilien~~ce ***in line with the climate goals set out in Regulation (EU) 2021/1119***. ***To that end, the site shall be able to meet as close as possible to 100 %, from locally produced, zero-emission renewable sources. Where meeting its entire demand from such sources is not technically achievable, the remaining demand may be met from other sources,***

through grid-connected supply, storage, flexible demand or contracted supply, provided that this delivers measurable emission reductions and benefits to the electricity system. Requirements shall be proportionate to the project and shall not make the designation conditional on continuous local generation where this is not technically achievable;

(j) the availability of water resources and the level of water stress in the area concerned.

(k) the expected impacts on, and benefits for, the local communities concerned, including as regards land use, noise, local employment, the reuse of waste heat by households and public facilities, and local public revenue.

(l) the contribution of the zone to a balanced geographical distribution of data centre capacity within the territory of the Member State.

1a. Member states shall ensure the impact analysis and its subsequent reviews for an acceleration zone is made publicly available upon request. Member states shall also ensure early communication and public-transparency protocols for local communities, including coordinated information sessions on the economic impacts and environmental measures before the designation of an acceleration zone, with a view to strengthening local acceptance and to identifying local communities needs.

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

(a) ~~conduct, and~~ review at least every three ~~years, a comprehensive~~ ***year current and future acceleration zones, and assess the impact based on the*** analysis of ***mentioned in paragraph 1 regarding*** the energy needs and their respective impacts on greenhouse gas emissions, of current an~~d future acceleration zones~~ ***the impact on air, noise and water pollution*** and identify the required energy ***and water*** infrastructure capacity ***and use*** for the proper functioning and development of data centre projects located in the acceleration zones. Such analysis ***Member States*** ~~shall be~~ conducted, at least, whe~~n designating the acceleration zones pursuant to paragraph 1;~~ ***also review the social and economic impacts of those data centres, including on public health, employment and tax revenue.***

(ab) ensure that the designation of acceleration zones does not exclude or disadvantage the development or expansion of data centres outside those zones, or restrict the access of such projects to general simplification measures available under applicable law;

(b) ~~(n)~~ sure 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.

Demócrata

3. National,regionalandlocalauthoritiesresponsibleforpreparingspatialand 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.

3a. When designating and managing acceleration zones, Member States shall apply objective anti-speculation criteria regarding electricity grid connection. Grid-capacity reservations and administrative priority shall be subject to verifiable use-it-or-lose-it milestones. Any capacity reservation for which substantial progress in civil works or equipment procurement cannot be demonstrated within 18 months shall lapse automatically and be promptly reassigned to active projects on the waiting list.

3b. Anti-speculation milestones relating to the reservation of electricity grid capacity shall be public, verifiable and proportionate to the scale of the project. Before releasing a reservation for failure to meet the 18 months deadline, the competent authority shall give the holder an opportunity to be heard and shall take account of delays attributable to public authorities, the grid operator or force majeure. Release shall be carried out in accordance with applicable grid access and connection rules.

4. Whendesignatingaccelerationzones,MemberStatesshallensuretheinvolvementof and coordination among all relevant national, regional and local authorities and entities, including ***the municipalities on whose the acceleration zone is to be located,*** 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.

4b. Territorial or environmental assessments and baseline analyses conducted in the context of the impact analysis under paragraph 1 when designating an acceleration zone shall allow individual projects to reuse those studies. The reuse of prior territorial or environmental assessments shall not waive project-specific assessments required by Union law. Developers relying in good faith on complete and current official data shall not be held liable for errors solely attributable to the authority providing those data, without prejudice to the correction of environmental effects and the rights of third parties.

4b. Without prejudice to paragraph 1 of this Article, Member States shall be permitted and encouraged to jointly designate 'cross-border data centre acceleration zones' within their territories when all the requirements set out in this Article are fulfilled. The Commission shall facilitate such cooperation where necessary and publish best-practice guidelines latest 3 months prior to this Regulation coming into effect.

Article 10a Mutual benefit agreements

1. Member States shall ensure that data centre projects deployed in acceleration zones provide benefits for the local communities concerned. To that end, Member States shall encourage voluntary agreements between data-centre operators and local

authorities to maximise local economic benefits. Competent authorities shall specify the measures expected from data centre operators in the designation act of an acceleration zone to facilitate the drawing up of a mutual benefit agreements. Such measures may include:

(a) Making waste hear available to the local heating networks, public buildings or other local users;

(b) ***Commitments on local employment and training, including specialist technical training;***

(c) Financial contribution to a local fund, or a community benefit agreement concluded with the municipalities concerned;

(d) Priority access to computing capacity for local public bodies, research and education institutions and local SMEs;

(e) ***Local supply-chain development;***

(f) ***Contributions to shared municipal infrastructure;***

or any other measures identified as benefiting the local communities, pursuant the consultation referred in Article 10, paragraph 1a.

2. Such agreements shall not constitute disproportionate preconditions for the designation of acceleration zones.

3. Member States shall prepare templates for mutual benefit agreements, including best practices.

4. Member States may require a facilitator to aid the process. The facilitator may support access to information on rights and opportunities for communities and assist in identifying the most appropriate and equitable benefit sharing mechanisms responding to the needs of the affected communities and citizens. Member States shall proactively inform municipalities and local associations of the identity, role and means of contacting the facilitator and such information shall be made publicly available through the single contact point referred under Article 12. The Commission shall draft guidelines based on best practices from existing Union and national law to inform such processes.

Article 11

Conditions within acceleration zones

1. ~~When setting~~***Member States shall set*** sustainability requirements for data centres deployed in acceleration zones***, including minimum requirements on energy efficiency and water use. When doing so***, 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) ***(r) and, once established, the common Union~~~~ rating scheme for data centres***.

1anew. Member States shall ensure that data center operators make available to the competent authorities the information referred to in Annex VII to Directive (EU) 2023/1791, in accordance with that Directive, and, in addition, information regarding on-site energy generation, including behind-the-meter generation and secondary emergency energy sources (diesel generators, batteries), including their

operating hours and emissions, the use of chemicals and refrigerants for cooling technologies, and water sourcing and discharge, including the temperature of water discharged into surface water or groundwater. The additional information shall be transmitted prior to the start of the project and at least once per year after.

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.

The priority access referred in paragraph 2a shall not be considered discriminatory within the meaning of this paragraph. The Commission shall monitor anti-competitive and speculative conduct by data center providers operators in acceleration zones and inform Member States, where relevant.

2a. Member States shall ensure that, in each acceleration zone, data centre operators established in the Union that are not controlled, directly or indirectly, by a third country or a third-country entity benefit from the following:

a) for [60] days from the publication of the designation, only Union operators may submit expressions of interest, stating their control structure, the land area and grid connection capacity sought, and an indicative timeline;

b) each such expression of interest shall confer priority in the allocation of the land area and grid connection capacity it indicates, provided that the operator submits a comprehensive application under Article 13 within [4] months of the expiry of the period referred to in point (a); otherwise, the priority shall lapse;

c) where the acceleration zone exceeds [2] hectares, at least 30 % of its land area and grid connection capacity shall remain reserved for Union operators for one year from the publication of the designation. Capacity allocated under point (b) shall count towards that share.

Capacity not allocated under this paragraph shall be allocated in accordance with paragraph 2.

2b(new) Where a data centre operator deploying capacity within an acceleration zone offers colocation or hosting services to third parties, it shall, before allocating newly available capacity to any customer, first offer that capacity to enterprise customers established in the Union on fair, reasonable and non-discriminatory terms, for a minimum period of [60] days. This obligation shall not apply to capacity built and reserved for the operator's own exclusive internal use.

The deployed capacity, including the volume, technical specifications, and price or pricing methodology, shall be published through the single information point referred to in Article 12. Where no Union-established enterprise customer accepts the offer within the priority window, the operator may allocate the capacity to any other customer on terms no more favourable than those offered under the first subparagraph.

2c. Member States may provide additional, transparent, objective and non-discriminatory incentives, in accordance with applicable Union law, to support the development of secure, resilient and Union-sovereign data-centre and cloud capacity in acceleration zones. Such measures may facilitate permitting, infrastructure readiness, access to skills and investment

Democrata

partnerships, while preserving effective competition and the objectives of this Regulation.

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 ***shall*** ~~***shall***~~ 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.

1a. 1a. Member States with composite or decentralised structures may organise that point through competent regional authorities or other bodies, while ensuring a single operational contact point for each project.

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

(a) spatialplanningandbuildingpermits;

(b) environmental assessments, in accordance with Regulation (EU) 2026/XXXX [on speeding-up environmental assessments]; ***including assessments on noise or chemical pollution***

(c) authorisationsregardingwater***use,***abstraction,wastewaterdischarge,andheat

(d) utilisation and recovery;

compliancewithapplicableadministrativeandreportingobligations;

(da) early communication and public transparency protocols for local communities, including coordinated information sessions on the economic and environmental measures and impacts of the project with a view to strengthening local inclusion and acceptance;

(e) ***Complete, timely and accessible*** information to the public, with the aim of increasing public acceptance of the data centre project ***and the acceleration zone***;

(ea) publication of an indicative timetable of procedural steps and responsible authorities, together with a digital mechanism for tracking applications, without altering the constitutional allocation of competences or creating additional authorisations;

(f) applicationsforconnectiontotheelectricity,heatorcommunicationsnetworks, or to other relevant networks.

Demócrata

(f) applicable common Union scheme for rating the sustainability of the data centres operating in the acceleration zone, in accordance with Delegated Regulation 2026/3472.

2a. Each single information point shall maintain a publicly accessible register of the data centre projects in the acceleration zones within its competence. The register shall indicate, for each project, the stage of the permit-granting procedure and shall contain an aggregated version of the information made available pursuant Article 11 (1) (new). The aggregated version shall contain all relevant information and allow citizens to understand the impact on the area concerned.

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.

4a. The single point of contact shall serve as contact point for the public and municipalities and set up a complaint handling mechanism for issues raised. A yearly report shall be drawn up for monitoring purposes and shall be submitted to the competent authorities upon request.

Demócrata

Article 13

Facilitating administrative and permit-granting processes

1. Datacentreprojectsdeployedinaccelerationzonesshallbeconsideredasstrategic 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. Foreachdesignatedaccelerationzone***,onthebasisoftheimpactanalysisreferedto in Article 10, paragraph 1***, 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.

2a. The competent authorities shall arrange for environmental, planning, industrial-safety and electricity-grid access authorisations to be processed simultaneously and in parallel. Administrative or judicial challenges concerning the delimitation of an acceleration zone shall not have suspensory effect on the processing of licences for individual projects that comply with the approved zone plan.

3. Beforeissuingtheaggregatedbaselinepermitreferredtoinparagraph2,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***, and the public participation required under Union law***.

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***, including the extension or modernisation of existing data centres,*** 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 ***be completed within a maximum period of*** 12 months, from the moment a comprehensive ***The period shall begin when the competent authority confirms that the*** application has been submitted ***is complete. Requests for additional information and suspensions of the time limit shall be reasoned, notified in writing and limited to strictly necessary elements. The procedure shall respect environmental assessment, public participation and effective judicial protection obligations. Where the technical, structural or environmental complexity of an application objectively so requires, the competent authority may grant one reasoned extension of no more than three additional months***. 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.

5a. The permit-granting procedure and the time limit referred to in paragraph 5 shall also cover the permits required for additional renewable electricity generation and energy storage facilities that are co-located with, ot located in proximity to, a data centre project deployed in an acceleration zone and intended to supply that project, and for the direct lines within the meaning of Article 2, point (41) of Directive (EU) 2019/944 connecting those facilities to the project, including where they serve as a bridging source of power pending connection to the electricity grid.

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 ***four*** 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~~ ***is*** highly sustainable ~~or~~ ***and includes*** innovative features, including technologies and solutions developed under Title II;

(ba) The project upgrades existing data center facilities by delivering significant sustainability improvements;

(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 systemoperator, inparticularfor projectsinvolvingthecolocationoflargeclean energy generation and storage facilities;

(ca) the project demonstrates significant contribution to the stability, resilience and decarbonisation of the electricity system, including demand-side flexibility, co-located energy storage or long-term clean-energy power purchase agreements (PPAs);

(cb) the deployment of high-performance computing and artificial-intelligence infrastructure addressing critical capacity shortfalls in underserved regions or supporting essential Union productive sectors;

(d) the project supports the integration of chips, processors and accelerators, servers or quantum computers designed***, developed*** and/or ~~m~~anufactured in ***wholly or in a substantive part within*** 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 ***provided that the project demonstrates a verifiable contribution to Union technological capability, industrialcooperation, security ofsupplyorvaluecreation***;

(da) the project demonstrates a verifiable contribution to strengthening Union data centre supply chains and reducing Union strategic dependencies in critical infrastructure inputs, including cooling and thermal management systems, power distribution and management systems, and other essential supporting infrastructure, through investment in Union manufacturing capacity, supplier diversification, or long-term supply agreements with Union-established producers, provided that this criterion shall not be construed to restrict the participation of international investment in data centre development or to impose local content obligations on project promoters;

(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***, and provides demonstrable benefitsforthe local communitiesconcerned***.

2. In its proposal, the applicant shall provide all the necessary and relevant information to demonstrate that the project fulfils the relevant criteria***, including information on expected and actual electricity consumption, peak demand, load profiles, electricity sourcing, including on-site and behind-the-meter generation and the fuels used, direct operational emissions, grid impact, water use, waste heat reuse potential, embodied emissions, hardware turnover, material requirements and the expected categoriesof usesupported bythe project***.

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.

3a. Projects designated as data centre strategic projects shall enjoy access to relevant Union financing instruments under the Connecting Europe Facility, Horizon Europe and the European Competitiveness Fund. Such projects shall furthermore be regarded as contributing to an objective of common interest for the purposes of State aid assessment, with a view to expediting the Commission's assessment of compatibility under Article 107 TFEU. However, designation as a strategic project shall not in itself confer an automatic entitlement to Union funding or a presumption of State aid compatibility. Applications for support shall continue to be assessed under the conditions of the relevant programmes and Articles 107 and 108 TFEU, while the project's demonstrated contribution to the objectives of this Regulation may be taken into account.

5. WheretheCommissionfindsthataprojectdesignatedasastrategicprojectnolonger fulfils the relevant criteria, or where its designation was based on an application containing incorrect information affecting compliance with those criteria, ***or where the project has not complied with its reporting obligations under Article 12 of Directive (EU) 2023/1791 and Delegated Regulation (EU) 2024/1364,*** 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.

6. Applications for recognition as a strategic project shall be assessed on the basis of objective, transparent and proportionate criteria. Third-country control or influence may be taken into account, provided that such assessment relies on verifiable evidence concerning beneficial ownership, voting rights or statutory decision-making powers. The nationality of board members, managers or staff lawfully resident in the Union shall not, in itself, constitute evidence of third-country control or influence. The Commission may withdraw designation following a reasoned assessment, after giving the project promoter an opportunity to be heard.

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) thecomputecapacityavailableintheUnion,includingedgecomputingcapacity;

(b) thevolumeofdemandfordatacentrecapacity***anditsutilisationrate***;

(c) thesizeofthecapacitygapandunderservedareasthatcouldbeidentifiedbythe Commission, in cooperation with the Member States, and subsequently used as acceleration zones for the deployment of data centre capacity***, and the geographical distribution of data centre capacity accross the Union***.

(d) the electricity consumption, peak demand, load profiles, electricity sourcing, including on-site and behind-the-meter generation and the fuels used, direct operational emissions, grid impact, water use, embodied emissions, hardware turnover, material requirements and expected workload growth associated with cloud, AI and data centre infrastructures, including infrastructures benefitting from public support, accelerated procedures or strategic status;

(e) The strategic dependencies affecting the Union's cloud and artificial intelligence ecosystem, including the critical technologies, infrastructure, services, and material capacity gaps that affect the Union's security of digital technology supply chains

The Commission shall make the findings of this assessment public and submit them to the European Parliament and the Council.

2. In exercising its monitoring functions, the Commission shall prioritise data already available under Union law and shall not impose reporting duties on data centre operators beyond those laid down in Union law, including under this Regulation. It shall publish comparable methodologies for installed capacity, utilised capacity and projected demand, distinguishing, where feasible, cloud, artificial intelligence and edge segments. The findings made public pursuant to paragraph 1 shall be presented in aggregated form so as not to disclose the identity of individual operators or their commercial customers, private contractual arrangements or trade secrets.

3. By [date of entry into force of this Regulation + two years], the Commission shall, in cooperation with the Member States, assess the opportunities for computing capacity located at different sites, including in different Member States, to be used jointly, in particular for the training of AI models across several sites. The assessment shall cover the electricity grid capacity available for new connections and the very high capacity networks within the meaning of Article 2, point (2), of Directive (EU) 2018/1972 connecting data centres, including across borders. The Commission shall make the assessment public, with due regard to public security, and may, on that basis, recommend measures to the Member States.

Denoland

TITLE IV
AUTONOMY
Chapter I
Cloud computing sovereignty framework
SECTION 1
UNION ASSURANCE LEVELS

Article 16
Scope

1. ThisChapterestablishesaUnioncloudcomputingsovereigntyframeworkcomprising 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. TheCommissionisempoweredtoadoptdelegatedactsinaccordancewith Article 45 to amend the Union assurance levels set out in Annex II and the evidence set out in Annex III. ***Such delegated acts shall not alter the four-level architecture, essential requirements or categories of adresses established by this Regulation, in particular by removing a criterion or an item of evidence, by narrowing its scope or by extending the possibilities of derogation from it. Any amendment having such effect shall only be made by the European Parliament and the Council on proposal from the Commission.***

3. ToensureAnnexIIandAnnexIIIremainuptodatewithnewlegalortechnical developments, the Commission shall review them at least every 18 months. ***The Commission shall submit the findings of this assessment to the European Parliament and the Council.***

Article 16a
Uniform application of the criteria

1. In order to effectively ensure correct, uniform and efficient implementation of the Union assurance levels, the Commission shall set out an appropriate methodology in a delegated act, by [P.O. insert date of entry into force plus 6 months]. The methodology shall set out clear criteria for the competent authorities designated pursuant to Article 25 and, where applicable, the Commission, to assess the application by a cloud computing service provider that aims to be recognised as offering a Union assurance level 2,3 or 4.

2. Member States shall ensure that their competent authorities apply the criteria set out in the methodology referred to in paragraph 1 in a uniform manner.

3. The Commission shall monitor the uniform application of the criteria set out in the methodology referred to in paragraph 1 on an annual basis and shall publish an

annual report on its findings, the first report being due one year after the entry into force of this Chapter.

4. Where the Commission has reason to believe that a Member State systematically does not apply the criteria set out in the methodology referred to in paragraph 1 in a uniform manner, in particular with possible impacts on the internal market and competition, it may investigate the matter on its own initiative. The Commission may take into account reasoned objections raised under Article 17.

5. Where, on the basis of its own investigation pursuant to paragraph 4, the Commission considers that a Member State does not apply the criteria set out in the methodology referred to in paragraph 1 in a uniform manner, it shall give that Member State the opportunity to submit its observations within a reasonable time limit. The Commission may then issue a warning to the Member State concerned. . The warning shall be a reasoned communication that:

(a) sets out the specific elements in respect of which the Member State does not apply the criteria set out in the methodology referred to in paragraph 1 in a uniform manner;

(b) specifies the measures that the Member State is to take to bring its enforcement into line with that methodology; and

(c) sets out a clear timeline within which the Member State is to take those measures, which shall be not less than [three] months unless the situation requires urgent action.

Where the Member State concerned has not taken the measures specified in the warning within that timeline, the Commission may, where appropriate and duly substantiated, temporarily suspend the ability of that Member State's competent authorities to recognise cloud computing service providers as offering a Union assurance level. The Commission shall not suspend that ability without having first issued a warning in accordance with this paragraph. The suspension shall be lifted as soon as the Member State has taken those measures.

6. The Commission shall coordinate with the Member States concerned in order to swiftly implement necessary measures that concern the uniform application.

7. Where, following the suspension, the Member State concerned fails to implement measures to ensure uniform application of the Union assurance levels, the Commission shall temporarily step in and take over the recognition of cloud computing service providers. The conditions set out in Article 17a shall apply.

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 ***responsible pursuant*** ~~***responsible pursuant***~~ ***to Article 25(4), or where Article 17a applies, to the Commission***. When submitting an application for recognition, the cloud computing service provider shall include all the relevant evidence required under paragraphs 3 or 4. ***The application shall identify the service concerned and its critical subcontractors. For each critical subcontractor, the application shall identify its material functions, relevant access rights, operational***

dependencies and any sub-outsourcing arrangements that may materially affect the security, continuity or sovereignty of the recognised service. Evidence already available through recognised Union certifications or registers shall not be requested again where it is relevant, current and sufficient

1a. Recognition shall be determined by the criteria applicable to the audited service and requested Union assurance level. The nationality of a shareholder that does not confer effective control, privileged access or another relevant legal exposure shall not, of itself, justify refusal of recognition. This paragraph shall not derogate from the ownership and control requirements expressly applicable under Annex II.

2. Thecompetentauthorityofestablishmentshallbetheevaluatingnationalcompetent authority. An evaluating ***Where an application is submitted to a*** national competent authority ***pursuant to paragraph 1,*** 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 nationalauthority that has received a request for collaborationshall either provide confirmation that it agrees to collaborate with ***be*** the evaluating nationalcompetent authority***. Where an application is submitted to the Commission pursuant to Article 17a, the Commission shall be the evaluating authority***or refuse the request.

For Union assurance level 1, the candidate cloud computing service provider shall submit to the evaluating nationalcompetent 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 nationalcompetent authority.

4. ForUnionassurancelevels2,3and4,thecandidatecloudcomputingservice provider shall submit to the evaluating nationalcompetent 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. Within60daysofacceptinganapplicationpursuanttoparagraph1,theevaluating national competentauthority 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 ***or, where relevant, the Commission*** 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 ***evaluating authority shall ensure that the recognition is in line with Article 16a on uniform application of the applicable criteria. Where the competent authorities of the other Member States or, where applicable, the Commission have reasons to believe that the recognition is not uniform and in compliance with Article 16a it shall submit a reasoned objection referenced under paragraph 6. 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

Demócrata

(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 evaluating competent authority's evaluation within 30 days. The evaluating competent authority shall take due account of those comments when ~~finalising~~ its conclusions. ***The evaluating authority shall acknowledge completeness of the application within 15 days; any request for additional information shall identify the missing evidence and suspend the applicable assessment period.***

5. During the review period referred to in paragraph 5, point (a), the national competent authority of another Member State***, or the Commission,*** 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. ***The reasoned objection or request for clarification shall be based on the metholdogy set out under Article 16a.***

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, ***and the Commission,*** 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***, or the Commission*** 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 d~~raft decision***, taking duly account of the criteria for uniform application of criteria for recognising Union assurance levels***. The evaluating national competent authority shall inform the competent authorities of the other Mem~~ber States~~***, and where relevant the Commission,*** 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 n~~ational competent a~~uthority may refer the matter to the Commission. The Commission shall assess the referral and may request information

from the national competent authorities concerned***, where applicable***. 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~~ ***shall suspend*** 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. ***The evaluating authority may lift the suspension, where it finds that cloud computing service provider has implemented necessary measures or revoke its recognition indefinitely. The evaluating authority shall immediately inform other Member States, and where applicable, the Commission, of the suspension and provide information.***

12. The Commission may adopt implementing ***delegated*** acts concerning the practical arrangements for the procedures referred to in this Article. Those implementing ***delegated*** 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 establishmentprovide, 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. When sending a request for information, the Commission shall state the purpose of the request, specify what

14. information is required and set the period within which the information is to be provided.

Demócrata

Article 17a
Commission as evaluating authority

1. By way of derogation from Article 17(1) and (2), the Commission shall be the evaluating authority for the recognition of a cloud computing service provider as offering Union assurance level 2, 3 or 4 only where:

(a) the provider operates in more than one Member State, the Member State in which the provider has its main establishment pursuant to Article 25(4) has conferred on the Commission the task of acting as evaluating authority in accordance with paragraph 3, and the provider has chosen to submit its application for recognition to the Commission in accordance with paragraph 2; or

(b) the Commission takes over the recognition of cloud computing service providers pursuant to Article 16a(7), in accordance with paragraph 4.

2. Where the conditions set out in paragraph 1, point (a), are met, a cloud computing service provider may choose to submit its application for recognition to the Commission instead of the national competent authority referred to in Article 17(1). The provider shall demonstrate in its application that it provides the service in the Member States concerned and shall inform that authority of its choice. A provider shall not submit an application for the same service to both the Commission and a competent authority.

3. A Member State may confer on the Commission the task of acting as evaluating authority for applications for recognition submitted by cloud computing service providers that have their main establishment in that Member State and operate in more than one Member State. The Member State shall notify the Commission of the conferral in writing, specifying its scope, in particular whether it covers all or only certain Union assurance levels among levels 2, 3 and 4, and the date from which it takes effect. The Commission shall confirm the conferral in writing and shall publish it in the register referred to in Article 25(2). From that date, the Commission shall act as the evaluating authority within the scope of the conferral, including for the suspension and revocation of recognitions under Article 17(11), for those providers that have chosen to submit their application to the Commission pursuant to paragraph 2. The Member State may withdraw the conferral by giving the Commission [six] months' written notice. Applications pending before the Commission at the date of withdrawal shall be completed by the Commission.

4. Where the Commission takes over recognition pursuant to Article 16a(7), it shall act as the evaluating authority for applications for recognition submitted to the competent authorities of the Member State concerned. It shall also act in that capacity for the suspension and revocation of recognitions granted by those authorities under Article 17(11). The Commission shall end the take-over once it has established that the Member State concerned ensures the uniform application of the criteria set out in the methodology referred to in Article 16a(1).

5. Article 17 shall apply mutatis mutandis where the Commission is the evaluating authority, with references to the evaluating authority read as references to the Commission. The competent authorities of the Member States may submit reasoned objections and requests for clarification during the review period referred to in Article 17(5), point (a). Article 17(10) shall not apply. Where the Commission intends to maintain its draft decision despite a reasoned objection, it shall adopt its final decision after consulting the competent authorities that submitted the objection.

6. The national competent authority referred to in Article 17(1) shall assist the Commission in the performance of its tasks under this Article and shall provide any relevant information without undue delay. Article 17(13) shall apply.

Article 18
Associated third countries

The Commission may adopt decisions, by means of ~~implementing acts~~ ***delegated acts in accordance with Article 45***, 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) itissubjecttoarelevantadequacydecisionadoptedunderArticle45of 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) itmaintainsanopenmarkettoUnioncloudcomputingservices;

(f) the thirdcountrygrants equivalentlevelsofaccesstopublicprocurement proceduresof cloudcomputingservicessubjecttothecontrolofaUnion 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)***. The assessment shall consider effective control, enforceability of safeguards, foreign-government access risks and continuity of service, and shall specify any conditions applicable to the relevant assurance levels.***

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. ***Except where immediate action is necessary to address a serious risk, the Commission may provide a reasoned transitional period where strictly necessary to ensure the continuity of essential services for Union entities and public sector bodies and assess continuity impacts before suspending or withdrawing the decision. That period shall normally not exceed [six] months and shall not be extended. Where the Commission establishes, on the basis of a documented migration plan and after consulting affected competent authorities, that a longer period is indispensable to prevent serious risks to essential-service continuity or data integrity, it may grant one reasoned extension limited to the time strictly necessary. No transition shall be granted where an immediate serious security risk requires suspension.***

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

Democrata

Article 19

Conformity self-assessment

1. Cloudcomputingserviceprovidersseekingrecognitioninaccordancewith 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. ***The self-assessment shall be service-specific and supported by a standardised declaration and evidence proportionate to Union assurance level 1.***

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. Cloudcomputingserviceprovidersseekingrecognitioninaccordancewith 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~~ ***approved auditor or audit firm***. 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. ***The audit shall be limited to the service and controls relevant to the assurance level sought. Approved auditors or audit firms shall take account of equivalent, current and independently verifiable evidence, such as cybersecurity certification schemes, without treating such certifications as automatic proof of sovereignty.***

2. Audited providers shall cooperate with auditing organisations ***the approved auditors or audit firms*** 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 ***The approved auditors or audit firms*** 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 ***approved auditors or audit firms*** shall only share

Demócrata

information that are necessary for the reporting purposes and do not contain any information that could reasonably be considered confidential.

4. Auditsreferredtoparagraph1shall***only***beperformedbyauditingorg~~anisations~~ ***approved auditors or audit firms which are approved by the competent authority of a Member State*** that:

(a) areindependentfrom,anddonothaveanyconflictsofinterestwith,thecloud computing service provider concerned, and any legal person connected to that provider, in particular:

i. havenotprovidednon-auditservicesrelatedtothemattersauditedtothe 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. havenotprovidedauditingservicespursuanttothisArticletothecloud computing service provider concerned or any legal person connected to that provider in the 10 ***3***-year period before the beginning of the audit; ***for the purposes of this point, independence shall be assessed on the basis of documented checks of actual and potential conflicts of interest, effective separation of incompatible services and appropriate rotation or independent review arrangements proportionate to the risk and duration of the audit engagement. An auditor shall not accept or continue an engagement where independence cannot be ensured by effective safeguards;***

iii. arenotperformingtheauditinreturnforfeesthatarecontingentonthe result of the audit;

~~(b) haveprovenexpertise,technicalcompetenceandcapabilitiesinauditingcloud computing services;~~

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

4a. Each Member State shall designate the competent authority to be responsible for approving auditors and audit firms. Member States shall only approve auditors and audit firms that:

(a) fulfill mutatis mutandis the conditions laid down in article 3 paragraph 3 and 4 of Directive (EU) 2006/43;

(b) are of good repute;

(c) have proven expertise, through educational qualifications or equivalent long-term practical experience covering technical competence and capabilities in auditing cloud computing services, particularly in the applicable criteria outlined in Annex II; educational qualifications in this regard shall include practical training and having passed an examination of professional competence of university final or equivalent examination level, organised or recognised by the Member State;

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

Democrata

their public-interest function, their integrity and objectivity and their professional competence and due care.

Member States may decide that auditors and audit firms that have been approved as statutory auditor or audit firm within the meaning of the Audit Directive 2006/43/EC and in addition fulfill the condition of proven expertise, can be considered approved as well under this Regulation.

4b. Member States shall ensure that, when the approved auditor or audit firm carries out the audit, they maintain professional scepticism throughout the audit, recognising the possibility of a material misstatement due to facts or behaviour indicating irregularities, including fraud or error. For the purposes of this provision, 'professional scepticism' means an attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement due to error or fraud, and a critical assessment of audit evidence.

4c. Each Member State shall ensure that approved auditors and audit firms are entered in a public register.

5. ~~Auditing organisations~~ ***Approved auditors and audit firms*** 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) thename,addressandpointofcontactoftheprovidersubjecttotheaudit,andthe period covered;

(b) thenameandaddressoftheauditingorganisationororganisationsperforming the audit;

(c) adeclarationofinterests;

(d) adescriptionofthespecificaspectsaudited,andthemethodologyapplied;

(e) adescriptionandasummaryofthemainfindingsdrawnfromtheaudit;

(f) alistofthethirdpartiesconsultedaspartoftheaudit;

(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) wheretheauditopinionis'negative',operationalrecommendationsonspecific measures to achieve compliance and the recommended timeframe to achieve compliance;

(i) wheretheauditopinionis'positive',theUnionassurancelevelthatneedstobe recognised under Article 17, issued to the audited service of the audited provider pursuant to the applicable criteria set out in Annex II.

5anew Where the audited provider is subject to a recognised EU or national cybersecurity or GDPR certification scheme, approved auditors and audit firms may rely on information from such certifications wherever the requirements and scope are equivalent or higher for relevant parts of the audit.

6. Where the ~~auditing organisation~~ ***approved auditors and audit firms*** was unable to audit certain aspects or to express an audit opinion based on its investigations, the

Demócrata

audit report shall include an explanation of the circumstances and the reasons why those aspects could not be audited.

7. Theauditingorganisation***approvedauditorsandauditfirms***mayrevokeitsaudit report and audit opinion where the audited provider, intentionally or negligently, supplied incorrect or misleading audit evidence.

8. Theauditedprovidershallannuallysubmitforreviewtheauditreportandthe associated 'positive' audit opinion to the same or a different auditing organisation ***approved auditors and audit firms*** which shall assess the continued compliance of the audited service with the applicable criteria set out in Annex II. ***The annual review shall focus on material changes and critical controls, a full reassessment shall be required only where those changes materially affect the level recognised or where justified by risk.*** On the basis of the annual review, the auditing organisation ***approved auditors and audit firms*** may confirm, update, or revoke the initial audit report and audit opinion.

9. TheCommissionisempoweredtoadoptdelegatedactsinaccordancewithArticle45 to supplement this Regulation by laying down rules on the performance of audits on the procedural steps, rules for auditing organisations ***approved auditors and audit firms*** and their technical competences, auditing methodologies and templates for the audit reports.

9anew Where access to third-party proprietary source code is legally or technically unavailable, the approved auditors and audit firms may accept independently verifiable alternative evidence, including controlled testing, attestations and contractual safeguards, provided equivalent assurance is demonstrated.

Article 20a
Support for SMEs and AI innovation

1. Member States and the Commission may establish support schemes, including audit vouchers, covering a substantial part of the cost incurred by providers that are SMEs or small mid-caps with genuine establishment and substantial economic activity in the Union and not subject to the control of a third country or of a legal entity established in a third country in obtaining their first recognition at Union assurance level 2, 3 or 4. Eligibility shall reflect objectively verifiable capability, additionality and the scope of the service to be recognised. The beneficiary shall in all cases meet every ownership, control, cybersecurity and sovereignty requirement applicable to the assurance level sought.

2. National competent authorities shall designate a contact point to provide guidance to SMEs and small mid-caps on the preparation of applications for recognition under Article 17, on the basis of the model audit plans and standardised evidence templates referred to in paragraph 3.

3. Member States shall provide a proportionate, risk-based verification mechanisms and simplified guidance for SMEs. By [entry into force + 12 months], the Commission shall publish model audit plans and standardised evidence templates adapted to SMEs.

3 a new The Commission may publish non-binding guidance on Member State investment incentives for European cloud and AI capacity, subject to the Treaties, State aid rules and applicable tax competences; eligibility shall be based on objective investment and capability criteria.

Democrata

Article 21

Content and quality of audit evidence

1. To prepare the audit report and audit opinion, the ~~auditing organisation~~ ***approved auditors and audit firms*** 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. ***The assessment shall rely on evidence that is necessary, relevant and proportionate to the requested level, avoiding duplication with evidence already independently verified under applicable Union law.***

For specialised cybersecurity functions, alternative technical controls may be accepted, provided that equivalent assurance is demonstrated and where they demonstrably preserve the required sovereignty outcome, ensure incident response and do not permit uncontrolled access to protected data.

2. The audit evidence shall be:

(a) relevant and sufficient to enable the auditing organisation ~~***approved auditors and audit firms***~~ to prepare an audit report and provide an audit opinion; and

(b) reliable, according to the auditing organisation's ***approved auditors and audit firms'*** professional judgment and scepticism.

2 a new. Where a subcontractor involved in the provision of the audited service operates a cloud computing service that is registered in the central repository referred to in Article 22 as recognised at the same or a higher Union assurance level, the auditing organisation shall accept that recognition as sufficient audit evidence in respect of the criteria of Annex II already covered by that recognition, and shall not require the audited provider to reproduce that evidence. The audited provider shall remain responsible for the criteria applying to its own layer of the service.

2 b new. The Commission shall, by means of implementing acts adopted in accordance with Article 46(2), recognise certification schemes for cloud computing services whose requirements are equivalent to or more stringent than one or more criteria of Annex II, and identify the criteria they demonstrate, provided that the scheme requires independent third-party audit and periodic re-audit and provides for the suspension and withdrawal of certificates. Only schemes established or overseen by a public authority of the Union or of a Member State may be recognised. A valid certificate issued under a recognised scheme shall be accepted as evidence of compliance with the criteria it is recognised as demonstrating; the auditing organisation shall verify its validity and scope and assess the remaining criteria. The Commission shall list recognised schemes in the central repository. Recognition of a cybersecurity certification scheme shall not in itself establish conformity with an ownership, foreign-law exposure, jurisdictional control or operational-autonomy criterion unless that precise criterion falls within the independently verified scope of the recognised scheme.

Demócrata

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'). ***The repository shall specify the scope, validity and assurance level of each recognised service and provide machine-readable access without disclosing protected security-sensitive information.***

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 ***not later than 30 days after that service has been recognised***.

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 ***immediately*** 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. ***Notifications shall primarily concern changes materially affecting recognised sovereignty controls and shall be coordinated, where practicable, with notifications required under other applicable Union cybersecurity legislation***

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 ***immediately***, 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) thenature,gravity,scaleanddurationoftheinfringement;

(b) anyactiontakenbytheinfringingpartytomitigateorremedythedamagecaused by the infringement;

(c) anyprevious infringements bytheinfringingparty;

(d) thefinancialbenefits gainedorlosses avoidedbytheinfringingpartyduetothe infringement, insofar as such benefits or losses can be reliably established;

(e) anyotheraggravatingormitigatingfactorapplicabletothecircumstancesofthe case;

(f) infringingparty'sannualturnoverinthepreceding financialyear inthe 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 obligationsunderthis Chapter.

Democrata

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 ***without prejudice to Article 16a(7) and Article 17a***. To that effect, Member States may designate an existing authority or existing authorities ('competent authorities').

2. MemberStatesshallnotifytheCommissionofthenamesofthecompetentauthorities and of their tasks and powers***, and of any conferral or withdrawal of conferral pursuant to Article 17a(3)***. 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 ***and with complete independence***. Member States shall ensure that their competent authorities have all necessary resources to carry out their tasks, including sufficient technical, financial and human resources ***as well as the premises and infrastructure necessary*** to adequately supervise all cloud computing service providers within their competence. ***Those resources shall also be sufficient for tasks carried out in the context of mutual assistance and cooperation.***

3anew 3a (new). The member or members of each competent authority shall, in the performance of their tasks and the exercise of their powers under this Regulation, remain

free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody. They shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

3 b new Member States shall ensure that each competent authority chooses and has its own staff, which shall be subject to the exclusive direction of the member or members of the competent authority concerned.

3 c new. Member States shall ensure that each competent authority is subject to financial control which does not affect its independence, and that it has separate, public annual budgets, which may be part of the overall state or national budget.

3e. new Where the Commission acts as evaluating authority pursuant to Article 17a, it shall perform its tasks and exercise its powers under this Chapter in an impartial, transparent and timely manner, and shall ensure that the requirements set out in paragraphs 3 and 3a apply to it and to the members of its staff carrying out those tasks, with the necessary adaptations. The Commission shall ensure that the staff carrying out those tasks do not receive instructions from, and are not subject to the influence of, any cloud computing service provider.

3f. (new) Member States shall ensure that their competent authorities cooperate with the Commission in the performance of its tasks under Articles 16a and 17a and provide it, without undue delay, with the information necessary for the monitoring, investigations and reporting referred to in Article 16a. This applies in particular where a Member State has conferred on the Commission the task of acting as evaluating authority pursuant to Article 17a(3).

Democrata

4. ~~The~~***Without prejudice to Article 16a(7) and Article 17a, 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. ***The authority of the main establishment shall act as the coordinating contact point for cross-border supervision, without prejudice to the powers expressly conferred on other competent authorities, or the Commission.***

Article 26

Powers of the national competent authorities

1. Where needed to carry out their tasks under Article 1~~7, competent authorities~~ of ~~establishment~~ ***and 17a, the evaluating authority referred to in Article 17(1) and, where it acts as evaluating authority pursuant to Article 17a, the Commission,*** 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; ***requests shall be reasoned,***

limited to information necessary for the identified supervisory purpose and subject to applicable safeguards, such as Union legislation applicable to trade secrets and security-sensitive material.

(b) thepowertocarryout,ortorequestajudicialauthorityintheirMemberStateto 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) thepowertoaskanymemberofstafforrepresentativeofthoseprovidersorthose 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.

1a. Where the Commission needs an inspection of premises pursuant to paragraph 1, point (b), it shall request the national competent authority of the Member State in which the premises are located to carry out the inspection or to request a judicial authority of that Member State to order it. That authority shall act on the Commission's request without undue delay.

2 Whereneededtocarryouttheirtasksunder Article 17, nationalcompetentauthorities of establishment ***authority referred to in Article 17(1)*** shall have the following enforcement powers:

(a) thepowertoorderthecessationofinfringementsand,whereappropriate,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) thepowertoimposefines,ortorequestajudicialauthorityintheirMemberState to do so, for failure to comply with this Regulation, including with any of the investigative orders issued pursuant to paragraph 1;

(c) thepowertoimposeaperiodicpenaltypayment,ortorequestajudicialauthority 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.

2a. Where a Member State has conferred on the Commission the task of acting as evaluating authority pursuant to Article 17a(3), the conferral shall extend to the powers referred to in paragraph 2. In that case, the Commission shall exercise those powers within the scope of the conferral in respect of cloud computing service providers that have submitted their application to it, and the national competent authority shall not exercise them in respect of those providers.

3 Measurestakenby***the*** nationalcompetentauthoritiesofestablishment***and,where applicable, the Commission*** in exercising their powers listed in paragraphs 1***, 2 and 2a*** and 2shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement or suspected

Democrata

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. ***The Commission shall exercise its powers under this Article subject to the same safeguards, in accordance with the Charter of Fundamental Rights of the European Union, and its decisions shall be subject to review by the Court of Justice of the European Union.***

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 ***including in the procedures under Articles 16a, 17 and 17a***. Mutual assistance shall include the exchange of information.

2. A competent authority ***or the Commission, where it acts as evaluating authority pursuant to Article 17a,*** 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 ***requesting*** ~~authori~~ty of establishment about ~~the action taken,~~ as soon as possible and no later than two months after receipt of the request, unless duly justified ***or within a shorter period set by the requesting authority where necessary to meet the time limits set out in Article 17. The requested authority shall use secure communication channels and may seek clarification where the purpose, scope or proportionality of a request is insufficiently specified, without unduly delaying urgent cooperation.***

3. The Commission shall, upon request, provide the national competent authorities with the information in its possession that is necessary for them to carry out their tasks under this Chapter, in particular the information necessary to assess draft recognition decisions of the Commission pursuant to Article 17 as applied by Article 17a, and information relating to conferrals pursuant to Article 17a(3).

Dornbracht

Article 28

Cross-border cooperation

1. Whereacompetentauthorityofdestination***ofanotherMemberState***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~~ ***responsible pursuant to Article 25(4)*** to assess the matter and to take the necessary investigatory and enforcement measures to ensure compliance. ***The request shall set out verifiable grounds for suspicion and the measures sought; any urgent protective action shall be reasoned and limited in scope and duration.***

2. TheCommissionmayalsorequestthe***national***competentauthorityreferredtoin ***responsible pursuant to*** Article 25 ***25(4)*** to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance***, except where the Commission itself acts as evaluating authority***.

3. Requestspursuanttoparagraph1or2shallbedulyreasonedandshallbedulytaken into account by the competentauthority of establishment ***receiving them*** . Where the competent ***receiving*** ~~authority~~ of establishmentconsiders that the information ~~provided is~~ insufficient, it may eitherrequest additional information. The period set out in paragraph 4 shall be suspended until that additional information is provided***.***

4. Thecompetentauthorityofestablishment***receivingtherequest***shall,assoonas 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 ***where it did not send the request,*** 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.

Democrata

4a new Where, in respect of a cloud computing service provider, the Commission acts as evaluating authority pursuant to Article 17a, a request of a competent authority of another Member State pursuant to paragraph 1 shall be addressed to the Commission. Paragraphs 3 and 4 shall apply mutatis mutandis, with references to the receiving authority read as references to the Commission.

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 ***or*** in the areas of national

security, internal security, external border management, defence, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal offence***, as well as the public sector activities listed in Annex IIa under Union assurance level 2, 3 or 4, irrespective of the administrative level or legal form of the public sector body or Union entity carrying them out***;

(b) determinewhichUnionassurancelevel2,3,or4setoutinAnnexIIofthis Regulation is appropriate for the identified public sector activities***, in accordance with paragraphs 1a***.

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.

The assurance level shall be determined for each service and intended use, having regard to the relevant risk. A public sector body or Union entity may accordingly use cloud computing services recognised at different Union assurance levels for different activities. The ownership or construction of physical infrastructure alone shall not trigger an assurance requirement. Cloud computing services provided by means of such infrastructure shall remain subject to this Article.

1a. The public sector activities listed in Annex IIa shall be assigned the Union assurance level indicated for them in that Annex. Where an activity falls under more than one Union assurance level in that Annex, the highest level shall apply.

By way of derogation from the first subparagraph , a Member State or Union entity may assign a different Union assurance level to a specific service, activity or identifiable workload where a documented assessment, applying the criteria in paragraph 2, demonstrates that the level is appropriate to the actual risks. The reasons for selecting the applicable level shall be documented and reviewable by the competent authority, without requiring publication of sensitive security information.

Member States and Union entities shall notify the Commission of each derogation under paragraph 1c, together with its reasons, within one month of its adoption. The Commission shall make the notified derogations available to the Member States through the cooperation referred to in paragraph 7.

For public sector activities not listed in Annex IIa, the selection of an assurance level shall be supported by a documented assessment of data sensitivity, service criticality, continuity needs and legal exposure, taking into account the aspects referred to in paragraph 2. The assessment shall not establish predetermined quotas for any level.

The Commission is empowered to adopt delegated acts in accordance with Article 45 to amend Annex IIa by adding public sector activities or by assigning another Union assurance level to an activity listed therein, in particular where derogations notified under paragraph 1d show that the level indicated in that Annex is not adequate. Delegated acts adopted pursuant to this paragraph shall be limited to technical updates of the descriptions of activities in Annex IIa and shall not amend the four-level Union assurance architecture, the essential criteria determining those levels or the scope of the obligations established by this Regulation.

2. Incarryingouttheirriskassessments,MemberStatesandUnionentitiesshallconsider at least the following aspects:

Demócrata

(a) thesensitivity,criticality,andmagnitudeofthenon-personaldataprocessed, 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) theriskandconsequentimpactonpublicorderofunlawfulaccessunderUnion law to such data by a third country or a legal entity established in a third country; theriskandconsequentimpactonpublicorderofpossibleservicedisruption;

(c)

(d) the risk and consequent impact on public order of organisational dependency on the service, including whether the entity would retain the independent human capacity to perform, verify or restore the supported public sector activity in the event of loss, degradation or malfunction of the service.

3. The Commission shall***, no later than 12 months after the entry into force of this Regulation***, 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. ***The methodology shall allow documented reliance on existing assessments under Directive (EU) 2022/2555 and, where applicable, Regulation (EU) 2022/2554, without treating cybersecurity compliance as automatic proof of sovereignty.***

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 ***a higher*** Union assurance levels ***level*** 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. ***The period may be extended to up to 24 months, on the basis of a documented migration plan, where strict compliance would create a material risk to continuity of essential services, security or data integrity.***

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 ***assess*** whether a multi-vendor or multi-cloud strategy is appropriate as part of their

Democrata

procurement of cloud computing services.

Article 30
Public procurement

1. ThisArticleappliestocontractingauthoritiesthatprocurecloudcomputingservices 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. Unionentitiesandpublicsectorsbodieswhosepublicsectoractivitieshavenotbeen identified as contributing to the preservation of public order under the risk assessment referred to in Article 29(1)***, or to which Union assurance level 1 applies under Article 29(1b),*** shall use cloud computing services that have been recognised under Article 17 as having ***at least*** a Union assurance level 1. ***Where no recognised service is reasonably available for the relevant workload, the contracting authority may apply paragraph 4 subject to a published, proportionate justification.***

3. Contractingauthorities,includingtheentitiesactingontheirbehalf,whoseactivities 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, ***or to which Union assurance level 2, 3 or 4 applies under Article 29(1a),*** shall only procure cloud computing services that have been recognised as having a ***the*** Union assurance level 2, 3 or 4 ***determined for the activity concerned under Article 29, or a higher Union assurance level***.

3a. Where a contract is divided into lots, the applicable Union assurance level shall be determined for each lot separately, in accordance with the risk assessment referred to in Article 29. Contracting authorities shall not aggregate lots in a manner that excludes providers that are SMEs or small mid-caps from participation without objective justification. A group of economic operators submitting a joint tender may demonstrate the applicable Union assurance level jointly, provided that each member of the group meets the criteria of Annex II in respect of the part of the service it delivers.

4. Byderogationfromparagraphs2or3,onanexceptionalbasisandwheredulyjustified, 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) thesubjectmatterofthetendercannotbesuppliedbyrecognisedcloud 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) thecontractingauthorityhaslaunchedasimilarprocurementprocesswithinthe previous year but did not receive any suitable tenders or suitable participants***, provided that the absence of suitable tenders or suitable participants did not***

result from an artificial narrowing of the procurement parameters;

(c) applyingtherequirementsofthisRegulationwouldrequirethecontracting authority to procure services at disproportionate cost. ***the procurement documents may allow tenders for cloud computing services not recognised at the required Union assurance level. Such a tender may be awarded the contract only where the contracting authority has demonstrated, on the basis of a reasoned assessment of security, continuity and life-cycle cost, that the lowest offer for a recognised service entails disproportionate cost. The contract shall provide for effective compensating safeguards, a fixed review date and the shortest feasible duration***

The decision shall specify the relevant workload, duration, safeguards and a review date. It shall not amount to a general exemption for the provider or contracting authority.

4a. Paragraphs 2 to 4 shall apply to each cloud computing service used to perform the contract, including where it is supplied through a reseller, integrator or managed service provider. The contracting authority or Union entity shall record in the repository referred to in Article 22 the provider of each such service and the reference to its recognition under Article 17 or, where paragraph 4 applies, the ground relied upon.

5. Contracts for cloud computing services shall permit the procuring entity to terminate without penalty where, following a change of control, the service ceases to be recognised at the Union assurance level required for the activity concerned.

Democrata

SECTION 2
PRIVATE SECTOR ENTITIES

Article 31
Impact assessments

1. Entities referred to in Annex I ~~of~~ ***to*** Directive (EU) 2022/2555 ~~who~~ ***that*** are not public sector bodies ~~may~~ ***shall, as part of their cybersecurity risk-management measures under Article 21 of that Directive and not as a separate procedure,*** carry out similar assessments as those set out in Article 29 ***to assess whether specific services, operations, activities or identifiable workloads relying on cloud computing services are critical to the continuity of essential services, public security or public order and, on that basis, whether Union assurance level 2, 3 or 4 is necessary and proportionate. The assessment shall take account of the nature and sensitivity of the data, the consequences of disruption or unauthorised access, the dependence on the cloud service concerned and the effective role of that service in supporting the critical activity. Inclusion of an entity in Annex I to Directive (EU) 2022/2555 shall not, of itself, determine the assurance level applicable to all its activities.***

1a. From [date of application + 3 years], where an assessment under paragraph 1 identifies a specific service, operation, activity or identifiable workload as requiring Union assurance level 2, 3 or 4, the entity concerned shall use cloud computing services recognised at least at the identified level solely for the cloud services and workloads that materially and directly support that identified critical activity. This

obligation shall apply only to contracts concluded or renewed after that date. Contracts concluded before that date may continue without alteration until they expire, but no longer than [two] years from that date. Where no appropriately recognised service is available on reasonable terms, the entity may use another service, provided that it documents the reasons, the risk assessment and appropriate mitigating measures. Union assurance level 1 shall not apply to entities covered by this Article.

1b. The identification of a critical activity shall not extend the corresponding Union assurance requirements to the entity as a whole, or to unrelated commercial activities, internal administrative functions, cloud environments or workloads that do not materially support the identified critical activity. Where infrastructure is shared between critical and non-critical activities, compliance may be demonstrated by effective technical, organisational or contractual segregation, provided that the safeguards applicable to the identified critical activity are not undermined. For all other activities, this Regulation shall not require those entities to use cloud computing services recognised at any Union assurance level.

1c. Financial entities within the meaning of Regulation (EU) 2022/2554 shall perform the assessments under paragraph 1 within their ICT risk-management framework under Article 6 of that Regulation. Assessments and relevant compliance evidence already prepared under Directive (EU) 2022/2555 or Regulation (EU) 2022/2554 shall be taken into account, without duplicative assessment, audit or reporting requirements. Supervision shall remain with the competent authorities designated under the respective instruments.

2. The Commission may***, after consulting the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 and, as regards financial entities, the European Supervisory Authorities established by Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010,*** issue guidance on the methodology for carrying out the impact assessments under this Article and possible ***additional voluntary*** 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

Demócrata

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. ***Without prejudice of paragraph 3, such criteria shall assess objectively verifiable contributions, including investment, research, skills, interoperability, supply-chain diversification and value creation within the Union, irrespective of the tenderer's place of incorporation.***

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.

2a. The non-price award criteria referred to in paragraph 1 shall together account for no less than 20 % of the total weighting of the award criteria. Within that share, the weighting of each criterion referred to in paragraph 3 shall be proportionate to its relevance to the subject-matter 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. ***Equivalent auditable contributions to resilience, interoperability and secure supply shall be taken into account where Union-designed components are not reasonably available.***

(e) the tenderer demonstrates effective operational autonomy, secure continuity, contractual enforceability and the capability to control, maintain or replace critical

Democrata

components of the service, including where the intellectual property rights necessary to operate, maintain or further develop the service can be exercised from within the Union, taking into account the risks of third-country interference and without prejudice to the ownership or control criteria applicable under Annex II for the assurance level required;

(f) the tenderer contributes to the maintenance of open source components used in the provision of the service, including through upstream contributions, irrespective of where the open source project concerned is hosted or governed;

(g) the service allows the contracting authority to migrate to another provider without disproportionate cost, through documented, machine-readable export of data and configuration, using open standards and interfaces.

(h) the extent to which the tendered service enables the contracting authority to obtain and export, in an open and verifiable format, evidence of actions performed by AI systems on its behalf, including the authority under which each action was performed, such that the evidence can be verified without the further cooperation of the tenderer.

4. The Commission shall, by [entry into force + 12 months], adopt implementing acts in accordance with Article 46 (2), specifying common indicators and evidence requirements for Union added value criteria.

Demócrata

Article 32a
Union assurance level at the award phase of the public procurement

1. In public procurement procedures for cloud computing services, contracting authorities may include, as part of the quality evaluation of the tender, a non-price award criterion that allows them to evaluate the Union assurance level of the service offered, as recognised in accordance with Article 17. They may do so irrespective of the activities or functions for which the service is procured.

2. Where contracting authorities apply the award criterion referred to in paragraph 1, they shall ensure that it:

(a) is expressly set out, together with its weighting and scoring method, in the procurement documents or in the contract notice;

(b) reflects the degree to which assurance levels demonstrably improve the security and resilience of the service for the intended use; and

(c) accounts for no more than 25 % of the total weighting of the award criteria.

3. The application of this criterion shall comply with applicable procurement law. It shall be considered to be linked to the subject-matter of the contract.

Article 33

Monitoring of procurement of innovation in cloud and AI

1. Member States shall monitor and report ***annually*** on their use of procurement of innovation in cloud computing services and AI systems. ***The report shall be submitted to the Commission and held in a central register.***

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. ***The monitoring shall include measurable participation by SMEs and scale-ups, the use of lots, portability requirements and the proportion of contractacts awarded to new market entrants.***

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) thesizeoftheeconomicoperatorsparticipatinginsuchprocurement;

   (b) SMEsparticipationtrends,includingthenumberofcontractsawardedtoSMEs, their share of the total contract value, as a percentage, and, where available, the share of cross-border SMEs participation;

   (c) measurestakentoimproveSMEsaccesstopublicprocurementprocedures.

   (d) the number and value of contracts for cloud computing services awarded to providers that are not subject to the control of third-country or of a legal entity established in a third country, and to other providers;

4. Member States shall pursue as objective that at least ~~25%~~ ***35%*** 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) preliminarymarketconsultations;

   (b) matchmakingbetweenpublicbuyersandinnovativesolutionsprovidedby European SMEs and start-ups;

   (c) developmentofpubliccontractclausesthatarefavourableforinnovativeSMEs.

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

Democrata

entities and public sector bodies on a voluntary basis. Union entities and public sector bodies may request the Commission to join the EuroCloud Federation. ***Participation shall not require the exclusive use of a particular supplier, technology stack or hosting model and shall preserve the autonomy of participating public bodies.***

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) acatalogueprovidinginformationonavailablepublicsectordatacentreservices and cloud computing services;

(b) aserviceplatformfortheexchangeandorchestrationofcomputing,storageand 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. ***Sharing arrangements shall specify responsibility for security incidents, data protection, service continuity, portability and termination, without prejudice to applicable Union law.***

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.

Demogata

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. ***The methodology for calculating fees shall be transparent, proportionate to actual administrative costs and shall not disadvantage smaller participating entities.***

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).

Demócrata

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. ***Where technically and economically appropriate, the procurement shall be structured into interoperable lots to enable participation by SMEs, scale-ups and specialist providers.***

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) actingasawholesalerbyacquiringsuchservicesandsuppliesandresellingthem 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) technicalinfrastructureenablingparticipatingentitiestouseawardedcontracts or award contracts, including specific contracts under concluded framework agreements, for data centre services, cloud computing services, software and AI systems;

(b) adviceandsupportonpreparingandimplementingprocurementprocedures;

(c) preparationandconductofprocurementproceduresonbehalfof,orinthename of, the entities concerned;

(d) invoicingandotheradministrativeservicesrelatingtothecontractsawarded.

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.

7. Cloud computing services procured under this Chapter, including services through which software or AI systems are delivered, shall comply with Article 30. Article 39(1) shall not affect that obligation.

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

Democrata

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. ***Accession conditions shall be published in advance, proportionate and designed to avoid excluding smaller contracting authorities solely on grounds of purchasing volume.***

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

Democrata

Article 37.

11. TheSteeringCommitteeshalladoptitsrulesofprocedure,followingaproposalfrom the Commission.

Article 38a

Committed purchases

1. Participating entities may, under the agreement referred to in Article 38, commit to purchase a minimum volume of cloud computing services, software or AI systems for funded activities assigned Union assurance level 3 or 4 under Article 29. That minimum shall not exceed [60] % of the estimated value of the procurement.

2. Committed purchases shall be awarded under the applicable procurement rules, where possible to at least two economic operators not under common control. The services shall be recognised at the Union assurance level assigned to the activity; the commitment towards an operator whose recognition is withdrawn shall lapse. Volume beyond the committed minimum shall remain open to competition, including to operators recognised after the award.

3. The procurement documents shall set requirements on service levels, switching and price, verified annually. Prices shall be assessed against those paid for services at the same Union assurance level outside the committed purchases. An operator that fails those requirements shall lose part of its committed volume, as provided in the procurement documents.

4. Committed purchases shall confer no entitlement to subsequent contracts.

Demócrata

Article 39

Applicable public procurement framework

1. Aparticipatingentityshallbedeemedtohavefulfilleditsobligationsunderapplicable 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. ***Such deemed compliance shall not relieve participating entities of obligations relating to data protection, cybersecurity, applicable assurance levels or contract management.***

2. TheproceduralprovisionsapplicabletoUnioninstitutionsshallapplytothe procedures for the award of specific contracts under framework contracts or dynamic purchasing systems.

3. Acontractingauthoritythathasacquireddatacentreservices,cloudcomputing 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. TheCommissionmaydecidetolaunchaprocurementprocedureopentoparticipating entities without a prior specific request from them.

5. BywayofderogationfromArticle168ofRegulation(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. ***Fee schedules and their calculation basis shall be published and reviewed periodically; fees shall not exceed the attributable costs of the procurement activities.***

5. 5. TheCommissionshalladoptimplementingactslayingdowndetailedrulesfor determining the fees, specifying the following:

(a) theestimatedcostsattributabletotheprocurementactivitiesforwhichfeesare chargeable;

(b) theindividualamountsofthechargeablefees;

(c) themannerandconditionsunderwhichthefeesaretobepaid;

(d) theconditionsunderwhichthefeesaretobepaid.

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

Democrata

Chapter V
Open source

Article 41

Promoting open source solutions and open source first

Such preference shall not constitute an obligation to select an open-source solution and shall not exclude proprietary or hybrid solutions where those solutions better meet objectively assessed functional, security, interoperability, continuity or total-cost requirements.

Before procuring a solution that is not based on open standards or components released under an open source licence, Union entities and public sector bodies shall document whether suitable open sources alternatives meeting the applicable security, functionality and total-cost requirements are available. Any published explanation shall respect the protection of commercially confidential information, intellectual property rights and information whose disclosure could prejudice cybersecurity or public security. Where they select such a solution, they shall record the reasons for that choice in the documentation of the procurement procedure, including, where applicable, the documentation referred to in Article 109 of Regulation (EU) .../... [Public Procurement Act], and make them publicly available. This assessment shall not create an obligation to select an unsuitable solution or favour a particular software licence solely by reason of its legal form.

Where Union entities and public sector bodies include requirements regarding the use of software released under open source licences, or of open standards, such requirements shall be presumed to be objectively justifiable for reasons of security and the prevention of vendor lock-in, and shall be considered functional requirements linked to the subject-matter of the contract within the meaning of Articles 88(3) and 90 of Regulation (EU) .../... [Public Procurement Act].

The Commission, in cooperation with Member States, shall establish contingency measures, including open source alternatives, to ensure the continuity of material functions of software widely used by Union entities or public sector bodies whose source code is not available under an open source licence, where that software can no longer lawfully or technically be provided, including as a result of export controls or sanctions.

Union entities and central government authorities within the meaning of Article 7(2) of Regulation (EU) .../... [Public Procurement Act] shall adopt, publish and update every three years an open source implementation plan, including an assessment of their dependencies on software not released under an open source licence.

~~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~~ ***shall, when defining their needs, specifications and award criteria for the procurement of cloud and AI solutions, or when developing such solutions, give preference, where technically feasible and relevant, to*** open standards and ***to*** components ***and solutions*** released under an open source licence***, including those available through the EU OSS Catalogue referred to in Article 43. In doing so, they shall take*** when ~~building their cloud and AI ecosystem or stack, takinginto account~~ functionalities ***functionality,*** includingsecurity~~, total cost~~***, including the cost of exiting the***

solution, and other relevant, duly justified objective criteria. ***In procurement procedures, that preference may take the form of specifications, award criteria or conditions for the performance of contracts, as referred to in Article 61(2) of Regulation (EU) .../... [Public Procurement Act], and shall apply irrespective of the value of the contract.***

Article 42

Share and reuse of software

~~When making~~ ***Union entities and public sector bodies shall make*** software to which they hold intellectual property rights***, including modifications to existing software,*** available for reuse under an open source licence, a Union entity or public ~~sector body shall do sousing a catalogu~~e or r~~epository t~~hat is connected to, and made accessible through, the EU OSS Catalogue referred to in Article 43.

Nothing in this Article shall require disclosure where doing so would jeopardise security, defence, personal data or the rights of third parties. Any publication decision shall respect applicable intellectual property and confidentiality obligations.

When commissioning software, contracting authorities are encouraged to consider securing reuse and portability rights proportionate to the intended public use, without requiring rights unnecessary for contract performance.

Demócrata

Article 43

EU Open Source Solutions Catalogue

1. TheCommissionshallprovideandmaintainanEUOpenSourceSolutionsCatalogue ('EU OSS Catalogue') as a centralised catalogue to access software made available for reuse by Union entities and public sector bodies.
2. TheEUOSSCataloguesshallbehostedontheInteroperableEuropeportalreferredto in Article 8 of Regulation (EU) 2024/903 and shall be accessible electronically free of charge.
3. TheCommissionshall,onthebasisofobjectiveandrelevantcriteria,decideonthe 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. ***Decisions shall be reasoned, based on published interoperable technical criteria, and subject to a proportionate review mechanism.***

4. Providers of open source solutions may request the inclusion of their solutions in the EU OSS Catalogue. The Commission shall decide on the basis of objective, transparent and non-discriminatory criteria, including the open source projects concerned. The catalogue shall indicate, where applicable, the Union assurance level at which a solution is offered as a cloud computing service.

Article 43a

Maintenance of critical open source components

1. The Commission shall identify, and review at least every two years, open source components on which the provision of cloud computing services and AI systems in the Union critically depends.

2. The Union shall provide funding, including from the programmes referred to in Article 6(3), for the maintenance, security remediation and long-term continuity of those components, in cooperation with open source software stewards within the meaning of Regulation (EU) 2024/2847 and with the OSPO Network referred to in Article 44.

3. In doing so, the Union and the Member States shall seek to maintain a critical mass of Union-based contributors to open source technologies of strategic importance to the Union's cloud and AI ecosystem, including technologies originally developed outside the Union, so as to ensure the ability to maintain, adapt, and, where necessary, independently continue the development of those components.

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) facilitatingtheexchangeofinformation,experienceandbestpracticesbetween 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) promotingthesharingandreuseofopen-sourcesoftwarebypublicsectorbodies;

(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;

(ca) facilitating secure maintenance, vulnerability disclosure, skills development and the participation of European SMEs and open-source communities.

(d) collaboratingonandexchangingopen-sourceprojectsofcommoninteresttoUnion entities and public sector bodies.

(e) advising the Commission on the identification of the components referred to in Article 43a (1).

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

Democrata

online.

Demócrata

TITLE V
FINAL PROVISIONS

Article –44 a new Reporting of infringements and protection of reporting persons

Directive (EU) 2019/1937 shall apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

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.

Democrata

Article 47

~~Review~~ ***Evaluation and review***

To ensure Annex II and Annex III remain up to date with new legal or technical developments, the Commission shall assess the need for amendment of the Union assurance levels set out in Annex II and the evidence set out in Annex III, once a year following the entry into force of this Regulation, and until the end of the period the delegation of power laid down in Article 44. The Commission shall submit the findings of that assessment to the European Parliament and the Council.

2. By [date of entry into force plus 4 years], and every 5 ***4*** ~~y~~ears thereafter, the Commission shall evaluate ***~~submit a~~ report on the evaluation and review of*** this Regulation, and report to ~~the E~~uropean Parliament, the Council and the European Economic and Social Committee.

The report shall include an assessment with regard to the structure of enforcement and the possible need for a Union agency to resolve any identified shortcomings. The report shall also assess:

(a) the share of public expenditure on cloud computing services for activities identified under Article 29(1) that goes to services recognised at Union assurance level 3 or 4;

(b) the number of such activities migrated to a service recognised at the required Union assurance level;

(c) the derogations under Article 30 (4) applied and renewed; and

(d) the concentration of suppliers for those activities;

The report shall be made public.

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 47a

Transitional provisions

1. A contract for cloud computing services used for activities referred to in Article 29(1), point (a), awarded under a procurement procedure launched, or a framework agreement or dynamic purchasing system concluded or set up, on or after [date of entry into force], may be terminated by the contracting authority or Union entity on three months' notice and without penalty where a risk assessment under Article 29 requires a Union assurance level that the service does not meet. The provider shall support migration within the period referred to in Article 29(6), in accordance with Chapter VI of Regulation (EU) 2023/2854.

2. From [date of application], Article 30 shall apply to any award, renewal or extension of a contract for cloud computing services, and to any modification extending its duration or scope, including under framework agreements or dynamic purchasing systems concluded or

Democrata

set up before that date.

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]. ***However, Article 47a(1) shall apply from [date of entry into force].***

This Regulation shall be binding in its entirety and directly applicable in all Member States.
Done at Brussels,

FortheEuropeanParliament
ThePresident

FortheCouncil
ThePresident

Demócrata

ANNEX I

GRAND CHALLENGES

1.GrandChallenge1: Environmentalsustainability,performanceandsecurityofthe Union'sdata 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) : 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.Themainfocal areasincludeenablingthe developmentof:
(c) advanceddatacentreenergyefficiencytechnologiessuchascooling,wasteheat
(c) recovery;
(c) quantum computing technologies for cloud and compute infrastructure
(c) operations;
gridintegration andadvancedenergymanagementsystems;
pilotlinesforthevalidationof next-generationenergy-efficienttechnologiesat operational scale.

(2) raisingaverageserverutilisationratesacrossthe Union's datacentres towards 50%, by integratingforexample,AI-poweredtechnologiesfordynamicserverutilisation management,runtimeworkloadmanagement andschedulingorforbalancing utilisation, energy cost, thermal constraints, and latency requirements.

(2) 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.

Pilotprogrammes couldhelpdemonstratethecapabilitiesoftheEuropeanopencloudstacksin strategically important sectors.

3.GrandChallenge3:FrontierAI

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.

Democrata

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.

Such approaches shall be assessed for their technical effectiveness, verifiable data isolation, output controls and protection of trade secrets, without creating a general obligation to pool commercially sensitive data.

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 resulting platforms should support traceable agent actions, revocable permissions, human intervention, secure interoperability and proportionate testing against misuse and cascading failures.***

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.

Democrata

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. Unionassurancelevel1

1.1. ForUnionassurancelevel1,cloudcomputingserviceprovidersmustmeetthe following cumulative criteria:

(a) thecloudcomputingserviceproviderisestablishedintheUnion;

(b) theinfrastructureandassetsofthecloudcomputingserviceprovider,includingthose 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) thecustomerdata,includingmetadataandtelemetrydata,thatisprocessed,storedand 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***. By way of derogation from point (c), where strictly necessary to detect, prevent or respond to cybersecurity threats and where that purpose cannot reasonably be achieved by processing within the Union, telemetry and operational metadata that do not contain customer data and from which customer data, or the identity or activities of individual customers, cannot be derived or inferred, associated with services recognised at Union assurance levels 1 to 3 may be processed outside the Union only to the extent necessary for that purpose, subject to appropriate technical, organisational and contractual safeguards. Such processing shall not permit access to customer content, shall minimise the risk of identifying sensitive customer activities, shall not make the data accessible to any third-country authority or entity that could compel its disclosure, and shall not undermine the assurance requirements applicable to the recognised service. The cloud computing service provider shall document the categories of data processed, the purpose, the location and the safeguards, and make that documentation available to the auditing***;

(d) wherethecloudcomputingserviceprovideroutsourcesthetechnicalandoperational 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***. Non-customer-specific threat intelligence and generic, non-operational technical advice shall not constitute technical or operational support of the audited service where they confer no access to customer data, privileged administration or operational control and cannot materially affect service security or continuity. This***

provision shall not exempt remote administration or operational support performed from outside the Union;

(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.

Union assurance level 2

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

2.1. the audited provider and the subcontractors which are involved in the provision of the audited service are established in the Union;

(a) 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;

(b) 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***. By way of derogation from point (c), where strictly necessary to detect, prevent or respond to cybersecurity threats and where that purpose cannot reasonably be achieved by processing within the Union, telemetry and operational metadata that do not contain customer data and from which customer data, or the identity or activities of individual customers, cannot be derived or inferred, associated with services recognised at Union assurance levels 1 to 3 may be processed outside the Union only to the extent necessary for that***

(c)

purpose, subject to appropriate technical, organisational and contractual safeguards. Such processing shall not permit access to customer content, shall minimise the risk of identifying sensitive customer activities, shall not make the data accessible to any third-country authority or entity that could compel its disclosure, and shall not undermine the assurance requirements applicable to the recognised service. The cloud computing service provider shall document the categories of data processed, the purpose, the location and the safeguards, and make that documentation available to the auditing;

(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. controlofthethirdcountryorthelegalentityestablishedinathird-countryover 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. accessbyathirdcountryorbyalegalentityestablishedinathird-countryto customer data is prevented;

iii. possibilityofdisruptionoftheservicecontinuityand/orthedegradationofthe service quality by a third country or a legal entity established in a third country is prevented;

iv. controlofthethirdcountryorthelegalentityestablishedinathird-countryover 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***. Non-customer-specific threat intelligence and generic, non-operational technical advice shall not constitute technical or operational support of the audited service where they confer no access to customer data, privileged administration or operational control and cannot materially affect service security or continuity. This provision shall not exempt remote administration or operational support performed from outside the Union***;

(i) the audited provider demonstrates that the following software supply chain measures are in place:

i. acompleteandup-to-datesoftwarebillofmaterials(SBOM),asdefinedin 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;

Demócrata

ii. wheresoftwarecomponentsasdefinedinRegulation(EU)2024/2847Article3, 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. wherethecloudcomputingserviceproviderissubjecttothecontrolofathird 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;

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) totheextentthattheauditedproviderprovidesitsservicesgloballyandmaintainsa 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.

(k) ForUnionassurancelevel2,thesubcontractorsreferredtointhefirstparagraphmust besubcontractors thatarethirdpartiesthathaveadirectcontractualrelationshiptothe cloud computing service provider and that contribute to the provision and delivery of the cloud computing service.

3. Unionassurancelevel3

3.1. ForUnionassurancelevel3,cloudcomputingserviceprovidersmustmeetthe following cumulative criteria:

(a) theauditedproviderandthesubcontractorswhichareinvolvedintheprovisionofthe audited service are established in the Union;

(b) theinfrastructure,assets,andpersonneloftheauditedprovider,includingthoseofthe subcontractors which are involved in the provision of the service, are located in the Union;

(c) thecustomerdata,includingmetadataandtelemetrydata,thatisprocessed,storedand 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; ***. By way of derogation from point (c), where strictly necessary to detect, prevent or respond to cybersecurity threats and where that purpose cannot reasonably be achieved by processing within the Union, telemetry and operational metadata that do not contain customer data and from which customer data, or the identity or activities of individual customers, cannot be derived or inferred, associated with services recognised at Union assurance levels 1 to 3 may be processed outside the Union only to the extent necessary for that***

purpose, subject to appropriate technical, organisational and contractual

safeguards. Such processing shall not permit access to customer content, shall minimise the risk of identifying sensitive customer activities, shall not make the data accessible to any third-country authority or entity that could compel its disclosure, and shall not undermine the assurance requirements applicable to the recognised service. The cloud computing service provider shall document the categories of data processed, the purpose, the location and the safeguards, and make that documentation available to the auditing.

(d) the personnel, including the personnel of the subcontractors which are involved in the provision of the audited service are Union ~~citizens~~ ***residents who have undergone security screening in accordance with the law of the Member State in which they work,*** 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; ***For the purposes of this criterion, personnel-related requirements shall apply only to persons directly involved in the provision, administration or privileged operational control of the cloud service covered by the recognition. They shall not extend to the provider's workforce as a whole or to staff whose functions do not confer such involvement or control.***

(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. controlofthethirdcountryorthelegalentityestablishedinathird-countryover 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, resources, 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. accessbyathirdcountryorbyalegalentityestablishedinathird-countryto customer data is prevented;

iii. possibilityofdisruptionoftheservicecontinuityand/orthedegradationofthe service quality by a third country or a legal entity established in a third country is prevented;

iv. controlofthethirdcountryorthelegalentityestablishedinathird-countryover 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***. Non-customer-specific threat intelligence and generic, non-operational technical advice shall not constitute technical or operational support of the audited service where they confer no access to customer data, privileged administration or operational control and cannot materially affect service security or continuity. This provision shall not exempt remote administration or operational support performed from outside the Union***;

(i) the audited provider demonstrates that the following software supply chain measures are in place:

i. acompleteandup-to-dateSBOMandalistofidentifieddependenciesrelevantto the provision of the service are documented and made available to the auditing organisation;

ii. wheresoftwarecomponentsorproductsareprovided,owned,andlicensedbya 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. wherethecloudcomputingserviceproviderissubjecttothecontrolofathird 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;

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;

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**.** ***Non-customer-specific threat intelligence and generic, non-operational technical advice shall not constitute technical or operational support of the audited service where they confer no access to customer data,***

Democrata

privileged administration or operational control and cannot materially affect service security or continuity. This provision shall not exempt remote administration or operational support performed from outside the Union;

(i) the audited provider demonstrates that the following software supply chain measures are in place:

i. acompleteandup-to-dateSBOMandalistofidentifieddependenciesrelevantto the provision of the service are documented and made available to the auditing organisation;

ii. measuresinplacetoretaineffectivecontroloverthesoftwarecomponentsor 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 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.

Demócrata

Annex IIa

UNION ASSURANCE LEVELS APPLICABLE TO PUBLIC SECTOR ACTIVITIES PURSUANT TO ARTICLE 29(1)A

In accordance with Article 29(1a), the Union assurance level indicated below applies to the storage, processing, back-up and disaster recovery, including by AI systems provided as cloud computing services, of the data, and to the services, listed for that level, irrespective of the administrative level or legal form of the public sector body or Union entity concerned.

Union assurance level	*Risk the level is intended to address*	*Data and services to which the level applies*
Union assurance level 1 *Location and basic safeguards*	*Non-critical services: exposure of data to processing outside the Union and lack of transparency on subcontractors, where a brief outage does not bring an essential function to a halt and disclosure would not harm citizens or public order.*	*(a) institutional websites, information portals and non-critical services;* *(b) public information, open data and aggregated statistics;* *(c) low-risk administrative data that contain no personal data of citizens and no information whose disclosure is restricted under Union or national law.*
Union assurance level 2 *Resilience and enhanced operational autonomy*	*Public services whose disruption would significantly affect citizens, and access by a third country to personal data or confidential information held by public authorities.*	*(a) significant administrative procedures, including the procedures listed in Annex II to Regulation (EU) 2018/1724, and benefit case files;* *(b) administrative files containing personal data, such as personal identifiers and income;* *(c) records of pupils and students held by public education institutions;* *(d) confidential documentation of public sector bodies, other than classified information.*

Democrata

Union assurance level	*Risk the level is intended to address*	*Data and services to which the level applies*
Union assurance level 3 *High operational sovereignty*	*Services whose disruption or exposure could compromise essential public functions, or expose the most sensitive data of a large number of citizens to access, coercion or interference by a third country.*	*(a) critical health information, namely personal electronic health data in the priority categories referred to in Article 14 of Regulation (EU) 2025/327, processed by or on behalf of healthcare providers and bodies providing electronic health record services to insured persons under national law, including statutory health insurers;* *(b) records of affiliation, contributions, entitlements and payments held by social security institutions;* *(c) taxpayer and customs registers and the assessment and collection records of tax and customs administrations;* *(d) large sensitive public security datasets, namely case files of courts, prosecution services and law-enforcement authorities, and criminal records;* *(e) population and civil-status registers, and the issuance and management of notified electronic identification means and European Digital Identity Wallets;* *(f) emergency coordination, including the handling of emergency communications to the single European emergency number '112' referred to in Article 109 of Directive (EU) 2018/1972.*
Union assurance level 4 *Maximum strategic sovereignty*	*Strategic functions where the loss of control could seriously affect national security or essential State interests, including through third-country interference.*	*(a) classified intelligence and other information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, or at an equivalent national level;* *(b) national defence operations and the operations of intelligence and security services;* *(c) strategic cryptographic keys or capabilities protecting the data and services listed under this level.* *(d) crisis-management and continuity-of-government systems of central governments and Union entities.*

This Annex does not cover general office, communication and collaboration services used by staff, the Union assurance level of which shall be determined in accordance with Article 29(1).

The entries relating to classified information, defence, intelligence and security are without prejudice to Article 4(2) TEU and to Union and national rules on the protection of classified information, which may impose additional requirements or exclude the use of cloud computing services.

Pericrata

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. AuditcriterionA–Unionestablishment

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) Anyevidencedemonstratingthattheauditedproviderisincorporatedunderthelawof a Member State in the Union or otherwise constituted in line with company law of a Member State in the Union.

(2) Anyevidencethattheregisteredoffice,centraladministration,andmainestablishment of the audited provider is established within the Union.

(3) Theauditingorganisationshouldverifytheapplicable Unionlegalframeworkofthe 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. Theauditingorganisationshouldverifywhethertheproviderislegallyincorporatedin 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).

(4) Theauditingorganisationshouldverifythestableandeffectivepresenceintheunion of the audited provider. The auditing organisation should therefore verify that:

(a) EUphysicalofficesoroperationalpremisesexist(forexample,throughlease contracts, utility bills or property documents);

(b) permanentstaffislocatedintheUnionandthatcustomersupportoperationsare carried out in the Union (for example, through employment contracts, payroll records, personnel timesheets);

(c) contractualoperationsarehandledintheUnion(forexample,throughactivity management records, incident reporting records);

(d) bankingandaccountingfunctionsareexclusivelyintheUnion(forexample, through financial statements and statutory audit reports).

(6) Theauditingorganisationshouldverifythepresenceof EUMemberState establishment units or branches (for example, through lease contracts, utility bills, property documents, employment contracts, timesheets, payroll records or purchase orders).

2. AuditcriterionB–Locationofinfrastructure,assets,andpersonnel

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) Locationofinfrastructure

(a) Alistwithrelevantdetailsofthelocationoftheinfrastructureanddatastorage 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) AnyotherevidencethattheITinfrastructureislocatedintheUnionsuchaslease agreements, property deeds, maintenance contracts, service contracts, facility access logs.

(c) Networkdiagramsandarchitecturedocumentsillustratingtheexclusiveuseof Union-based infrastructure for data storage and processing, including backup and replicated data.

(2) Locationofassets

(a) Alistandrelevantdetailsoftheassetsusedintheprovisionoftheaudited service, such as an asset register.

(b) Evidencethatservers,equipment,andoperationalassetsarelocatedinthe 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.

(b) Evidencethatservicedeliverycapabilitiesarebasedintheunion,suchas deployment records, installation records, service status reports, configuration reports, monitoring outputs, admin logs showing usage of the service.

(3) Locationofpersonnel

(a) Alistandrelevantdetailsofthepersonnelinvolvedintheprovisionofthe audited service. Evidencethatthepersonnelinvolvedintheprovisionoftheauditedserviceare

(b) located in the Union, including employment contracts, payroll records, timesheets, activity records, and organisational charts showing Union-based staff with operational responsibilities.

(4) Considerationsregardingtheinfrastructure,assetsandpersonnel

(a) Theauditingorganisationshouldalsoassesswheresuchinfrastructure,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.

: '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. AuditcriterionC–DatalocalisationintheUnion

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) Evidencedemonstratingthatcustomerdataarestoredandprocessedexclusivelyinthe 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) Evidenceoflogsandmonitoringrecordsdemonstratingthatalldataarestoredand processed exclusively within the Union. Examples include master service agreements, data processing agreements, data residency contractual agreements or any EU data boundary.

(3) Evidence(suchascontractualagreements,logs,andproceduresofferedtopublic 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) nocustomerdata,includingencrypteddata,aretransferredoutsideoftheUnion without public sector body approval;

(b) nodataaretransferredtoanythird-partyotherthansubcontractors whichare involved in the provision of the service or recipients expressly authorised by the public sector body.

Democrata

(4) Adataflowdiagramshowingtheflowsofdatabetweenthecloudcomputingservice 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) inputintothecloudcomputingservicebyoronbehalfofthecustomer,including authentication credentials;

(b) producedthroughthecustomer'suseofthecloudcomputingservice.

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. AuditcriterionD–Unioncitizenship

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) Theauditedprovidershouldprovidetheauditingorganisationwithproofthatithas 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) Theauditedprovidershouldprovideorganisationalchartsandjobdescriptions 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) Theauditedprovidershouldprovidedocumentsdemonstratingaccesscontrolpolicies and audit trails showing that only authorised personnel who are Union citizens can access the service's systems and data.

(4) Theauditedprovidershoulddemonstratethatithasputinplaceproceduresdescribing how citizenship is verified before assignment and how compliance with this audit criterion is maintained throughout employment.

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. AuditcriteriaE–Europeancybersecuritycertificationschemeadoptedunder 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) AvalidEuropeancybersecuritycertificateissuedbyacompetentconformity 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) Acertificationreportincludingadescriptionofthemaincomponentsusedforthe development and operation of the cloud computing service that is covered by the audit certificate.

(3) UntiltheEuropeancybersecuritycertificationschemecoveringcloudcomputing 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) avalidcertificateissuedbyacompetentconformityassessmentbody(inline 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) intheabsenceofanationalscheme,evidencedemonstratingadherencetothe highest level of cybersecurity standards available on the market.

6. AuditcriterionF–AIsystemsoperatedbyathirdcountryorthirdcountrylegal 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) Contractualclausesstatingthatdataprocessedorgeneratedbyusingtheaudited 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) Contractualclausesspecifyingthatdataareprocessedsolelyforthedeliveryofthe audited service and not for service improvements or model or system enhancements or any other secondary purpose.

(3) Dataflowdiagramsdocumentingtheend-to-endflowofdata,coveringdataingestion, storage, processing and deletion. The diagrams should also show where the AI pipelines or machine learning operations (MLOps) connect with customer data.

(4) MLOpsordeploymentrecordsdemonstratingthatthebuild,testandreleaselocations are in the EU.

(5) Modelorsystemcardscoveringthemodelorsystemname,version,trainingand validation sources, including statements that the data generated by using the audited service does not leave the Union.

(6) Datalineagepolicesandrelatedimplementationdocumentationthatshowsthatthe provider operates data lineage and provenance tools and that can demonstrate (per record) what the data has been used for.

(7) Alistofthesubcontractors(indicatingtheircountryofestablishment)thataccessthe data generated by using the audited service. **AuditcriterionG–Absenceofthird-countrycontrolorthird-countryentity control**

7.

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) Theauditingorganisationshouldidentifyandanalyse:

(a) alldirectandindirectshareholders,uptotheultimateowners;

(b) thecaptabledocumentingthecompany'sownershipstructure;

(c) thebodyorbodiesempoweredtotakestrategicdecisions(generalassemblyof shareholders, supervisory board, board of directors, etc.);

(d) therulesfortheappointment/election/removalofgoverningbodiesandthe 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);

(d) thequorumsandmajorityrequiredforadoptingstrategicdecisions,inorderto 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) thepossibleinfluenceonstrategicdecisionsthroughcommerciallinks,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) thelocationandfulladdressoftheglobalheadquartersand/orheadoffice;

(b) thelocationsoftheexecutivemanagementstructures.

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

(a) Adetailedlistdescribinganyownersthat:

i. hold,directlyorindirectly,atleast5%ofthecapitaloratleast5%ofthe 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. haveoneormoreofthefollowingspecificrightsinrelationtotheir 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) Theauditingorganisationshouldrequestthefollowingsupportingdocumentsto assess the elements in paragraph 2(a):

i. commercialregistryextractsandshareholders'booksoftheorganisation 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. foranyshareholdersthatarelegalpersonsthatholdatleast5%inthe capital or at least 5% of the voting rights:

(3) agraphdescribingthedifferentownershiplayers/chainofcontrol until the ultimate owners;

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

(3) aregisterofdirectors,officersandsignatories.

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

(a) Theauditedprovidershouldprovidetheauditingorganisationwithadescription of:

i. thedecision-makingbodies,theircompositionaswellastheirnationality or place of establishment (where applicable);

ii. therulesregardingelection,appointment,nominationortenureof members of the decision-making bodies or other management positions;

iii. thedecision-makingprocedures,includinginformationontherequired

majority and/or quorum needed for decisions;

iv. internalgovernancepoliciesdescribinghowownershipandcontrol decisions are recorded and approved;

board and management decisions reflecting the stated control structure;

board minutes and resolutions for control changes.

(b) Theauditedprovidershouldprovidetheauditingorganisationwithsupporting 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) Theauditedprovidershouldprovidetheauditingorganisationwiththeevidence 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). The supporting

(a) 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) Thesupportingdocumentsshouldincludeloandocuments,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) Theauditedprovidersshouldindicatetotheauditedorganisationifthereisany 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) Supportingdocumentsshouldprovideevidenceofanysuchcontrolora 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.*

Democrata

7.2. Additionalstepsbasedontheconclusionoftheownershipandcontroltest

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) DemonstratingthattheCommissionhasadoptedadecisionpursuanttoArticle 19 regarding the third country for which the cloud computing service provider is subject to the control of;

(d) Allevidence demonstrating that the audited provider and 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) Allevidencedemonstratingthatthepublicsectorbodywillbeinformedofany such request and a confirmation that the request has been refused;

(f) Allevidencedemonstratingthemaintenanceofanup-to-daterecordofany 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. AuditcriterionH–NotechnicalandoperationalsupportoutsideoftheUnion

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) evidencethattheauditedproviderhasimplementedbindingcontractualclausesstating 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) evidencethattheauditedprovidermaintainsanup-to-datesubcontractorregister;

(3) evidencethattheauditedproviderdoesnotsubcontractortransfersuchactivities outside of the Union;

(4) evidencethattheauditedproviderhasimplementedthenecessarylegal,technicaland 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, 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) evidencethattheauditedproviderensuresthatthepersonneluponthedeparturefrom the company have no further access to the audited service and revokes all access policies;

(7) evidencethattheauditedproviderhasimplementedthenecessarytechnicaland 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) evidencethattheauditedproviderhasproceduresinplacethatthereisnoeffective control of a third country or a legal entity established in a third country, including for subsequent sub-outsourcing.

9. AuditcriterionI-Ensuringthetransparencyofthesoftwaresupplychain

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) Theauditedprovidershouldmakeavailabletotheauditingorganisationacomplete and up-to-date software bill of materials (SBOM) for all software components, including open-source software (OSS).

(2) Theauditedprovidershouldmakeavailabletotheauditingorganisationalistof dependencies. This should include:

(a) allsoftwaremodules,librariesorapplicationprogramminginterfaces(APIs) used, as well as development tools;

(b) originofsoftware:where(countryoforigin)andbywhomthesoftwareis designed, developed and maintained, the location and jurisdiction governing the software distribution, and updates; degreeofrelianceonnon-

(c) EUvendors,facilities,orproprietarytechnologies;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. degreeofrelianceonopen-sourcesoftware;

(d) visibility into the entire software manufacturer and sub-manufacturer chain,

(e) including audit rights.

Democrata

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) Theauditedprovidershouldprovide:

(a) evidenceofarisk-basedprocessforidentifyingandmitigatingdependencieson external software manufacturers relevant to the operation of the cloud computing service;

(b) evidencethatithasidentifiedoneormorealternativesoftwaresolutions, 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) evidencethatitcanmigratetoanalternativesolutionintheeventofanydefector failure of the vendor or restrictions from a third country or a legal entity established in a third country;

(d) providealistofopenstandardsthatarefollowedaspartoftheauditedproviders policies regarding the audited service;

(4) Theauditedprovidershouldensuretransparencythroughremoteaccessandsource code auditability by:

(a) makingavailabletotheauditingorganisationalistofevidencetoprovethatthere 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. evidencerelatedtothetestingofthesoftwarecomponenttopreventthe 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. evidencethattheorganisation'schangemanagementprocedurescover 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. evidencethatthemaintenanceprocedureisupdatedtoinclude preventing any remote feature or mechanism that could be used to materially tamper with or disrupt a device, system or software.

(b) Theauditedprovidermustensurethatthethird-partyindependentauditoris 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. AuditcriterionJ–Open-sourcesoftware

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) Theauditedprovidershouldensuretransparencythroughremoteaccessandsource code auditability by:

(a) makingavailabletotheauditingorganisationalistofevidencetoprovethatthere 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. evidencerelatedtothetestingofthesoftwarecomponenttopreventthe 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. evidencethattheorganisation'schangemanagementproceduresinclude 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. evidencethatthemaintenanceprocedureisupdatedtoincludepreventing any remote feature or mechanism that could be used to materially tamper with or disrupt a device, system or software;

(2) Theauditedprovidershouldprovide:

(a) evidenceofarisk-basedprocesstoidentifyandmitigate:(i)aweakecosystem 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. evidencethattheauditedproviderhasappliedtheup-to-dateOSSwithoutundue delay;

(b) evidencethattheauditedproviderhasidentifiedoneorseveralalternativeopen-source solutions. If the audited provider cannot identify an equivalent software, it

(c) 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) Whereetheauditedproviderusessoftwarereleasedunderanopen-sourcelicence,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. **AuditcriterionK–**

11. Globalservicesandsubsidiariesinthird-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) Theauditingorganisationshouldverifythatthesubsidiaryislegallyandoperationally independent from the audited provider.

(2) Theauditedprovidermustdemonstratethatthesubsidiaryhasnoaccesstosystems processing or storing the customer data.

(3) Theauditedprovidermustdemonstratethatthesubsidiaryhasnoprivilegedaccounts within the Union production environments, including cloud administration, Identity and Access Management (IAM), Privileged Access Management (PAM), monitoring or database administration privileges.

(4) Theauditingorganisationshouldverifythatthepersonnelofthesubsidiarycannot obtain access to Union customer data.

(5) Theauditingorganisationshouldverifythatthesubsidiaryhasnoauthoritytoinstruct 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.

Democrata