Connect Europe views on the Cloud and AI Development Act (CADA)

November 2026

Introduction

Connect Europe welcomes the proposed Cloud and AI Development Act (CADA). This timely and essential initiative reflects the European Commission's clear strategic vision: to significantly strengthen Europe's cloud, AI and digital infrastructure ecosystem. Europe's competitiveness, resilience and technological sovereignty depend on its ability to deploy, scale and operate cloud, edge, AI and data centre infrastructure at pace and at scale.

The proposal contains several welcome elements, including measures to accelerate infrastructure deployment, establish common European sovereignty criteria and use public demand to support Europe's cloud and AI ecosystem.

To turn this ambition into tangible growth and investment, the final framework should act as a catalyst for European cloud, telecommunications and digital infrastructure providers to deploy, scale and compete. This requires a balanced mix of enabling measures: faster and more predictable physical deployment, access to affordable low-carbon energy, sustained and accessible investment support, demand-side measures that create real market opportunities for European providers, ambitious but proportionate sovereignty requirements and a coherent regulatory environment that avoids unnecessary duplication and fragmentation.

Connect Europe, in the following paragraphs, will provide its comments aimed at further improving the CADA proposal, focusing on six pillars: Measures to foster capacity; Sovereignty level related considerations; Consistent and homogeneous application vis-à-vis other EU legislation; Potential indirect implications for other private-sector entities; Sustained investment support; Greater weight for sustainability, based on achievable criteria.

1. Measures to Foster Capacity

1.1 Facilitate cloud and AI infrastructure deployment across Europe

Connect Europe welcomes the promotion of increasing datacentre capacity. This can be achieved by increasing capacity in existing data centres and through Data Centre Acceleration Zones (DCAZ) with a focus on energy supply and grid connections. Connect Europe calls for DCAZs permitting and deployment simplifications to benefit digital infrastructure investment more broadly across the Union and measures aimed at the development of a

European cloud and edge-cloud ecosystem led by European electronic communications network and service providers.

Reducing permitting delays, improving administrative coordination and facilitating grid connections are essential steps towards closing Europe's computing infrastructure gap. DCAZs can contribute to these objectives and should be framed as a positive instrument supporting investment and faster deployment.

Nevertheless, Europe's infrastructure ambitions cannot rely only on projects located in designated zones. Limiting the benefits of accelerated procedures to such zones could create a two-speed deployment framework and leave relevant projects outside its scope. Moreover, there is a risk of crowding out strategically relevant projects due to the ability of a few large actors to mobilise resources in a way that smaller actors will struggle to compete with.

While the Regulation may support the timely deployment of infrastructure, it should avoid creating incentives that disproportionately favour large-scale, centralised deployment models, such as those associated with DCAZs. Facilitating measures should be technology-neutral and location-neutral and should be granted taking into account their value for EU resilience, technological sovereignty and the fact they respect sustainability requirements. The same considerations should guide the designation of data centre strategic projects under Article 14, in line with the link the proposal itself makes between data centre capacity and the Union's competitiveness, resilience and sovereignty (recital 36).

Such an approach, with multiple DCAZs, would better support the development of a competitive and resilient European cloud ecosystem. Moreover, building new data centres is not the only way to develop EU sovereign and sustainable cloud capacities, upgrading already existing ones is an essential lever of action. In that regard, the CADA should make clear that DCSPs and DCAZs could also cover the renovation and improvement of existing data centres.

The concentration of capacity within designated acceleration zones risks reinforcing existing market structures and attracting investment in a manner that may further consolidate the position of incumbent large-scale providers. Consequently, the benefits arising from such measures would likely accrue primarily to operators already established in the market. This concentration risk should also be reflected in the designation of Data Centre Strategic Projects under Article 14, with criteria that take account of a project's contribution to European technological sovereignty, provider diversity and resilient European-controlled cloud and AI capacity.

Conversely, European data centre operators and distributed edge-cloud architectures can help to diversify supply and provide performance characteristics, including low latency and proximity processing, that are indispensable for next-generation cloud and artificial intelligence applications and, more broadly, for the

long-term competitiveness of the European economy. To support these objectives, measures aimed at accelerating deployment should also facilitate the modernisation and reuse of existing telecommunications infrastructure.

In light of the above, and with a view to extending supporting measures also to edge cloud infrastructure, we deem that a new definition should be included in the Regulation for "cloud computing infrastructure", that covers both data centres[1] and edge nodes[2]. This new definition should replace the data centre focus in the articles regarding DCAZs and strategic projects.

The development of a European cloud and edge cloud ecosystem will rely to a significant extent on the active participation of European telecommunications operators because they:

- Already have many solutions in place, be it in the area of sovereign cloud or in the development of edge cloud services. In addition to providing connectivity services, many are actively commercialising cloud offerings and are themselves among the most intensive and rapidly growing consumers of cloud and AI services for network management, automation and operational purposes.
- Own and manage infrastructure assets that are not only indispensable to the functioning of current cloud architectures but are increasingly evolving towards new cloud-enabled use cases. In particular, traditional electronic communications sites and exchanges are progressively being repurposed as edge computing nodes, reflecting and facilitating the future evolution of cloud and AI services.
- Have a proven track record in the deployment of advanced technologies at scale, extensive geographical reach, the provision of highly resilient services, and effective cooperation with public authorities. Taken together, these characteristics make them uniquely positioned to contribute to the achievement of the objectives of the Regulation.

Connect Europe key requests

1*. Keep facilitating measures technology- and location-neutral, without favouring centralised models such as DCAZs, and take EU resilience, technological sovereignty and sustainability into account when granting them and designating data centre strategic projects under Article 14.*

2*. Add a definition for "cloud computing infrastructure" and take it as the new reference for supporting measures.*

3*. Recognise edge cloud as a strategic enabler of innovation, resilience and European competitiveness, and give priority to its development over policies primarily aimed at concentrating capacity within dedicated acceleration zones.*

[1] pursuant to Article 2 point (10) of the Regulation

[2] as defined in Article 2, point (6), of Decision (EU) 2022/2481 ('the Digital Decade Policy Programme 2030')

***4**. Recognise European electronic communications operators as key actors in the delivery of the Regulation's objectives and, accordingly, channel financial support, policy incentives and facilitating measures towards the transformation of distributed electronic communications infrastructure footprints into cloud and edge-cloud platforms capable of supporting the next generation of digital services, while promoting a brownfield-first approach that supports the modernisation and reuse of existing telecommunications infrastructure on an equal footing with projects located within DCAZs.*

***5**. Apply permitting simplification, effective one-stop-shop arrangements and predictable timelines to all data centre and edge-cloud projects across Europe.*

1.2 Make the availability of affordable low-carbon energy a strategic competitiveness priority

Connect Europe welcomes the recognition of energy as a strategic enabler. Delivering Europe's digital infrastructure ambitions requires access to affordable low-carbon energy across the Union as well as power availability, predictable connection times to the energy grid and solutions for grid congestion.

Energy availability is indispensable for infrastructure deployment, but availability alone does not provide a sustainable business case. Energy affordability remains one of the key unresolved challenges for the competitiveness of European cloud, AI and data centre infrastructure. To expand computing capacity while retaining and attracting investment, digital infrastructure operators must be able to access energy under competitive and predictable conditions.

This is particularly important as data centre operators face growing expectations on sustainability, energy efficiency and environmental performance. Where new obligations are introduced, for example on energy labelling and efficiency, they should be matched by an enabling policy environment and corresponding support that recognise their cost implications and facilitate investment in efficient infrastructure.

Energy affordability should not be treated as an issue only for Data Centre Acceleration Zones. It is a horizontal condition for cloud, edge, AI and data centre deployment throughout the Union and should therefore be addressed in a broader and more consistent manner.

This is particularly important as, despite the strategic role assigned to digital infrastructure, the sector still lacks structural measures to mitigate energy cost exposure or dedicated incentives at national or EU level. Ensuring predictable and competitive energy conditions is essential to make large-scale investment in European digital infrastructure economically sustainable. Therefore, Connect Europe invites policymakers to ensure that energy-related incentives and grid access measures apply not only to large-scale data centres but also to distributed

edge-cloud infrastructures, which are increasingly essential for low-latency AI applications, network resilience and European digital competitiveness.

An investment-friendly location policy is therefore a necessary condition for achieving the sovereignty and resilience objectives pursued under the CADA. Particularly in the data centre sector, electricity prices constitute a significant – if not the central – competitive factor and a key benchmark for a location's attractiveness. After all, electricity prices account for 30–50 per cent of data centre operating costs. An excessively high level of electricity prices, which is uncompetitive compared to international benchmarks, is therefore an obstacle to the development of a sovereign and resilient data centre infrastructure.

While the Commission has established a framework for electricity price relief for energy-intensive industries under the Clean Industrial State Aid Framework (CISAF), eligibility is primarily linked to sectors listed in the Climate, Energy and Environmental Aid Guidelines (CEEAG). Although CISAF allows unlisted sectors to qualify where the relevant eligibility criteria can be demonstrated, it remains unclear whether this pathway is practical and accessible for data centres in practice.

Even where their services are sourced externally, data centres are fully integrated into modern industrial companies, both virtually and in terms of value creation. They are therefore indispensable to the competitive business activities of companies in the economic sectors listed in the CEEAG. They control highly complex manufacturing processes and, through automation, enable gains in efficiency and accuracy that would not otherwise be possible. As such, data centres contribute significantly to the value added of the industries that depend on them. Accordingly, coherent support for the listed economic sectors must also extend to data centres.

Effective access to State aid for data centres under the CEEAG requires not only their inclusion among eligible sectors, but also a review of the trade- and energy-intensity criteria, which fail to reflect the sector's specific characteristics, growing energy needs and strategic importance. Furthermore, the special cost-reflective network tariffs complementing CADA similar to those envisaged under Article 18(3) of the *"Futureproof Electricity Bills" proposal*[3], should be accompanied by proportionate flexibility requirements and investment aid, potentially under a dedicated State aid framework, to enable investments in demand response, load shifting, storage and smart energy management, as tariff differentiation alone is insufficient.

Connect Europe key requests

[3] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/943, as regards future-proofing electricity bills in the Union, through reducing system costs and fostering electrification and digitalisation, COM(2026)600

***1**. Establish a clear legal framework for measures that support power availability for new data centre and edge cloud capacity and help European providers with electricity costs, for example in the context of strategic projects. The creation of acceleration zones is a good step in the right direction. However, their benefits, such as faster administrative and permit-granting procedures under Article 13, will only materialise if they attract sufficient investment in data centre and edge cloud infrastructure. Acceleration zones will fall short unless CADA also addresses high electricity prices.*

***2**. Review the existing state aid framework: include strategic projects within the meaning of Art. 14 CADA within the Climate, Energy and Environmental Aid Guidelines (CEEAG) framework, ensuring that support measures adequately reflect their contribution to European industrial competitiveness and resilience and adapt the eligibility criteria to reflect the specific characteristics of the data centre sector and its strategic role in driving digitalisation and enabling new digital services.*

***3**. Complement CEEAG reform with a dedicated State aid framework for data centres, notably to support investments in flexibility, including demand response, load shifting, energy storage and smart energy management, needed to access the conditional network-tariff arrangements envisaged by the proposed "Futureproof Electricity Bills" proposal[4].*

2. Ensure that the sovereignty framework remains ambitious and focused on the public sector

Connect Europe fully endorses the establishment of common European sovereignty criteria, provided that the framework remains risk-based, proportionate and operationally feasible.

We welcome the introduction of a multi-tier framework based on the critical nature of public services and data supported by procured cloud and AI solutions. Different use cases entail different risk profiles and safeguards and related requirements. Thus, we welcome that the framework preserves sufficient flexibility to accommodate a range of different cloud services depending on the criticality of the data involved.

We also consider the proposed cumulative approach appropriate: each tier builds upon the requirements of the previous one while incorporating additional conditions aimed at achieving higher degrees of technological and operational sovereignty. The architecture proposed by the Commission, with four differentiated levels and requirements that become progressively more demanding across the criteria set out in Annex II, should be preserved. The higher levels should not be diluted, and the pathway for associated third countries at level 3 under Article 18 should remain subject to all its cumulative conditions.

[4] Ibid.

Nevertheless, the provisions set out in the main text and Annex II are highly complex, burdensome and may allow for a considerable degree of interpretation. The framework does not appear fully aligned with the objective of regulatory simplification and risks generating legal uncertainty, notably because many of its key elements will only be defined through future implementing acts. Greater clarity is needed from the outset regarding

(i) the criteria and process by which cloud services are recognised as meeting a particular Union Assurance Level (Article 17), and
(ii) the factors that determine which assurance level is required for a given public-sector activity or use case (Article 29), as well as the practical consequences of each determination.

The framework should place stronger emphasis on the demonstration of effective control over the core components of cloud and AI services, assessed at the level of the individual service and proportionately to the Union Assurance Level sought. This is essential to ensure that sovereignty objectives are effectively achieved in practice, and that formal compliance alone does not lead to distorted assessment results. Effective control should be demonstrated where it is material to the risk profile of the service concerned. Requiring providers to own or control every upstream technology component, irrespective of risk, would be disproportionate and inconsistent with the cooperation models on which European providers legitimately rely.

While the framework indicates that Tier 1 should constitute the default and most widely used classification, responsibility for the assessment and classification of services rests with the Member States. However, beyond the establishment of certain timelines, the text does not provide sufficient detail regarding the methodology or criteria to be applied in carrying out such assessments.

The methodology should support sufficiently granular, risk-based assessments so that higher UALs apply only to the activities, use cases and supporting workloads that objectively require them, rather than indiscriminately to entire public bodies, sectors or service portfolios. A common EU methodology should support consistency without displacing Member States' responsibility for the final Union Assurance Level determination, particularly where public-order or national-security considerations are involved.

Guidance, risk-assessment methodologies and recognition procedures should be sufficiently clear to prevent divergent interpretations and disproportionate requirements. Conversely, the framework should not be diluted by excessive optionality that would undermine its credibility.

In addition, a harmonised approach can strengthen trust, reduce fragmentation and increase visibility for trusted European services. It can also support the growth of European cloud, connectivity and digital infrastructure providers by creating a clearer market for services meeting defined sovereignty requirements. Connect

Europe, therefore, encourages the Commission to refocus the criteria on substantive considerations rather than formal requirements, as well as further clarify the conditions applicable to each sovereignty tier in the final text. Reducing interpretative ambiguities would contribute to a more harmonised implementation across the Union and reduce the risk of compliance approaches that fulfil the requirements only in a formal sense, without effectively advancing the policy objectives of the framework.

Clarification in this area would also provide greater certainty regarding the range of cooperation models available to European providers that maintain commercial, technological or strategic partnerships with hyperscale providers, while preserving the framework's sovereignty objectives and fostering a competitive European cloud ecosystem. Without endorsing any particular commercial model, the final text should make clear that a range of arrangements, such as managed sovereign services, technology licensing, joint ventures and resale arrangements, remains available, provided the requirements applicable to the relevant Union Assurance Level, in particular on operational and legal control, are met.

For the CADA sovereignty framework, built on the Union Assurance Levels, to deliver a competitive advantage for European providers, the final Regulation should embed pragmatic and operationally workable principles into its core design. The final text should also clarify how the Union Assurance Levels relate to the Commission's Cloud Sovereignty Framework and its SEAL levels, already applied in EU cloud procurement, so that providers and contracting authorities face one coherent set of sovereignty criteria.

The sovereignty framework should focus on effective operational control, while taking relevant ownership, jurisdictional and geographical considerations into account to the extent justified by the nature and level of risk associated with the services concerned. Sovereignty requirements should therefore address, in a proportionate manner, the relevant dimensions of control over data, infrastructure, access rights, supply chains, legal exposure and continuity of service. This would help ensure that the framework strengthens trust and resilience without creating rigid requirements that are disconnected from the actual risk profile of different services and use cases.

Sovereignty assessments shall also duly consider the specific legal and regulatory environment in which providers and operators operate. Existing oversight frameworks for strategic players, including Golden Power, provide significant safeguards for the protection of strategic assets and critical infrastructure influence and constrain key governance decisions within the relevant entity, and, in practice, limit the possibility of deliberate access to data by third-country entities. These safeguards shall therefore form part of a holistic assessment of risk and effective ownership and control.

Building upon this proportionate structure, the sovereignty framework should strike a pragmatic balance by combining robust technical, cryptographic, and

operational protections, such as advanced end-to-end encryption, sovereign key custody, and strict access management, alongside necessary legal or geographical safeguards. This hybrid approach ensures that compliance requirements remain flexible, realistic, and commensurate with the actual level of security needed for the processed data. Technical and cryptographic safeguards can complement these criteria, but should not substitute for the ownership, jurisdiction and control requirements that define the higher assurance levels.

At the same time, to foster a highly predictable investment environment, it is critical that these specific compliance metrics and audit evidence remain stable over time. The European Commission should commit to a stable regulatory horizon, ensuring that any future revisions of the technical annexes are subject to thorough impact assessments developed together with market players. Given that Annexes II and III may be amended and are subject to periodic review, any change to sovereignty criteria or audit evidence should be accompanied by proportionate transition arrangements. Adequate implementation periods and protection against abrupt disruption for services already recognised under a given Union Assurance Level are necessary to protect long-term investment decisions.

This predictability must be paired with a targeted scope across the entire cloud supply chain to secure true operational control. Cloud services rely on complex, multi-layered ecosystems of software vendors, technology partners, hardware and firmware suppliers as well as sub-processors. The CADA framework should therefore identify which of these actors fall within the full scope of the Union Assurance Level requirements and which are treated as supply chain dependencies subject to proportionate assurance obligations. In particular, the notion of "subcontractor" used in Annex II should be clarified: so that subcontractors that are directly involved in providing the service and that can access to customer data are object of the requirement for the UAL classification are considered for the UAL classification. Notably, passive and non-operational data centre providers should fall outside this definition as they have no access to customer data, service layers or data-processing activities, exercise no control over customers' architecture or data flows and cannot materially disrupt the service. In such cases, customers retain operational control and can switch between colocation providers, meaning that these providers do not create the type of dependency that the framework seeks to address.

In addition, Annex II, level 3 point (d) and level 4 point (d), read with Annex III criterion D, currently extend citizenship requirements to a very broad group, potentially including management and developers without operational access.

EU citizenship and security clearance should only be required where the contracting authority's risk assessment demonstrates the need; generic management and development functions without such access should be excluded.

Market availability should also be considered when applying the framework. Sovereignty requirements should encourage investment and the gradual development of European alternatives while remaining implementable in practice.

Public procurement can play an important role in this respect, including through an appropriate weighting of Union added value criteria to provide incentives needed for the uptake of trusted European solutions. At the same time, the application of the framework should take due account of market availability. Contracting authorities must retain practical solutions where the market cannot supply an appropriate recognised service or where compliance would entail disproportionate costs. Derogations should be clearly defined and applied consistently, to preserve flexibility, procurement feasibility and the overall credibility of the framework.

When it comes to public procurement the Commission notes the dependency (three hyperscalers count for 70% of the Union market while the European providers keep 15% together). The Commission rightly recognises the importance of the public procurement to change this trend.

Connect Europe key requests

1. *Confirm the four Union assurance levels in Article 16 and the principle that public authorities must procure services appropriate to the sensitivity of the use case under Articles 29 and 30.*

2. *Confirm the proposed architecture of four differentiated levels, with requirements that become progressively more demanding. Do not dilute the higher levels.*

3. *Clarify that sovereignty assessments shall also duly consider the specific legal and regulatory environment in which providers and operators operate. Existing oversight frameworks for strategic players, including Golden power, provide significant safeguards for the protection of strategic assets and critical infrastructure influence and constrain key governance decisions within the relevant entity, and, in practice, limit the possibility of deliberate access to data by third-country entities. These safeguards shall therefore form part of a holistic assessment of risk and effective ownership and control.*

4. *Rely on public-sector signalling rather than private-sector mandates. Recital 66 already recognises that public procurement requirements influence regulated industries and generate market spillovers. Private companies have diverse risk profiles and are already subject to sectoral risk-management frameworks such as NIS2 and DORA. Recent private-sector tenders, including Airbus's "Trusted Cloud" procurement, demonstrate that demand for sovereign services can develop voluntarily.*

5. *Make public procurement an effective anchor market. The derogations in Article 30(4) must remain transparent and narrowly interpreted.*

6. *Keep Article 18 strict and evidence-based. Recognition of an associated third country for level 3 must remain conditional on all cumulative requirements in Article 18, including protection against unlawful data access and service disruption, open market access and public-procurement reciprocity.*

7. *Include a new article in the proposal by amending Art 30 to require the authorities that procure cloud computing services and choose a non-European provider to explain their reasons for selecting a non-European provider.*

8. *Simplify the recognition process and provide planning certainty by:*
- *Setting a deadline for auditors in Article 20 (i.e. 120 days)*
- *Limit delegated powers and stabilise the criteria and extend the review cycle - Article 16(2) should permit only technical updates to Annexes II and III, not fundamental changes to the logic or scope of the assurance levels. Article 16(3) should extend the review cycle to 36 months from current 18 months.*
- *Provide realistic migration periods. The maximum 12-month period in Article 29(6) should be extended to at least 24 months.*

9. *Amend to ensure Annexes II and III are operationally proportionate and clarify the concepts of 'subcontractor' and personnel "involved in the provision of the service". The definitions of relevant personnel, assets and subcontractors should use a materiality test based on access to customer data, including data in transit, or privileged access to the systems used to operate the service, including the ability to monitor, reroute or alter data flows. Only subcontractors directly involved in providing the service that meet this test should be considered for the UAL classification. Providers of physical infrastructure only, such as premises, power or cooling, should fall outside the scope.*

3. Deliver simplification through genuine regulatory coherence

Connect Europe calls for a simplification mindset to guide the legislative process and the implementation of CADA. This requires streamlined procedures within the Regulation itself and coherent interaction with existing and forthcoming European and national frameworks.

A European sovereignty framework can provide significant value if it replaces fragmented approaches with a predictable and commonly recognised system. It should not become an additional layer of requirements operating alongside substantially equivalent national or European certification, cybersecurity and compliance mechanisms.

The relationship between the CADA Assurance Levels and existing or future European cybersecurity certification schemes, notably the EUCS currently under development, should be clear and operational. The final framework must ensure that the intended delineation between technical cybersecurity requirements and sovereignty requirements results in genuine complementarity in practice and avoid duplicating certification, auditing, evidence or compliance obligations.

Additionally, the requirement for an annual review of the audit appears disproportionate and risks creating unnecessary administrative burdens and additional compliance costs for providers. A more balanced and proportionate approach would rely on less frequent periodic reviews, while maintaining a robust obligation on providers to promptly notify any material change in circumstances that could affect the validity of the audit findings or the recognised assurance level.

Where a service or provider has already been certified or audited under a recognised national or European scheme, the framework should provide for effective recognition of the relevant results. Recognition may need to account for differences in scope, but providers should not be required to repeat equivalent processes or produce the same evidence multiple times as certification and auditing procedures can be lengthy and resource intensive.

While CADA is intended to lead progressively to a common Union framework, where a service or provider has already been certified or audited under a recognised national or European scheme, the relevant results should be recognised to the extent that they provide equivalent evidence against the applicable CADA criteria. Existing schemes should be mapped against the Union Assurance Level criteria, so that each scheme is recognised for the requirements it covers. Providers should not be required to repeat equivalent processes or produce the same evidence multiple times, as certification and auditing procedures can be lengthy and resource intensive. This common European approach would provide cross-border legal certainty and spare providers from navigating competing or cumulative systems.

Finally, the respective responsibilities of cloud service providers and their hardware, software and other supply-chain partners should be sufficiently clear. Suppliers need predictability as to which requirements apply to individual components, who must demonstrate compliance and how evidence provided by different actors in the value chain will be assessed.

Connect Europe key request

1. *To ensure real simplification and timely effectiveness of CADA recognise existing certification evidence for cloud computing services during the transition to the common Union framework.*

4. Keep the sovereignty framework focused on the public sector

Connect Europe has identified the future application of the framework to private-sector entities as an issue requiring particular attention during the legislative process.

Article 31 currently allows private entities falling under Annex I of NIS2 to conduct assessments similar to those carried out by public bodies. It also empowers the Commission, in specified circumstances and through delegated acts, to require impact assessments and risk-mitigation measures for private entities operating in sectors of high criticality. Article 31(3) should be deleted. Private-sector entities should remain free to use the framework voluntarily, and CADA should not empower the Commission to impose mandatory assessments or mitigation measures on private procurement through delegated acts. This would also avoid overlap with existing sectoral risk-management frameworks such as NIS2 and DORA.

In any event, the framework should provide for the recognition and reuse of compliance evidence for entities already subject to other European regulatory frameworks, such as NIS2, DORA,while duly taking into account the security measures, oversight mechanisms and safeguards already imposed under applicable sectoral and national legislation.

Deleting Article 31(3) would enhance legal certainty and help preserve the ability of private-sector organisations to make technology and procurement decisions based on their operational and business needs.

Connect Europe key request

1. *Delete Article 31(3). Private-sector entities should remain free to use the framework and the Commission's guidance under Article 31(1)-(2), but the Commission should not be empowered to impose mandatory assessments and mitigation measures by delegated act. Recital 64 relies on the necessary and proportionate public-order exception in Article III:2(a) of the WTO Agreement on Government Procurement. This exceptional logic cannot simply be transferred to private procurement decisions.*

5. Match regulatory ambition with sustained investment support

Connect Europe calls for the Union's regulatory ambition to be matched by sustained and accessible financial support for research, deployment, scale-up and market creation.

European cloud, edge, AI and data centre capabilities require long-term investment covering research and development, commercial deployment and the scaling of solutions. Funding instruments should be predictable, efficiently administered and accessible to the range of actors contributing to the European cloud-to-edge ecosystem.

Regulatory and funding frameworks should support the competitiveness of strategic digital infrastructure investments across Europe and help accelerate the deployment of efficient technologies, while avoiding a situation in which new obligations are introduced without corresponding conditions for investment and competitive operation.

CADA's infrastructure and sovereignty objectives should not depend on funding that remains uncertain or fragmented across multiple programmes. The framework should maintain continuity with existing European initiatives while simplifying access, reducing delays and ensuring that financial support contributes effectively to deployment and market uptake.

Financial support should be complemented by demand-side measures that encourage the uptake of trusted European solutions and provide greater predictability for investors. Public procurement, long-term purchasing commitments and well-designed incentives can help translate Europe's strategic objectives into concrete market opportunities, while supporting the gradual scaling of European cloud, AI and digital infrastructure providers.

Supply-side funding must also be accompanied by demand-side measures. Long-term procurement commitments, increased uptake of European solutions and predictable market opportunities are necessary to establish sustainable investment cases and enable European providers to compete at scale.

Connect Europe key request

1. *Ensure that CADA is accompanied by sustained, predictable and accessible EU funding and demand-side measures that support research, deployment, scale-up and market uptake of European cloud, edge, AI and data-centre solutions.*

6. Prioritise data centres with sustainability features to benefit from the CADA mechanisms

Connect Europe calls for giving more weight to the sustainability criteria to benefit from the Data Centre Acceleration Zones (DCAZs) and Data Centre Strategic Projects (DCSPs) mechanisms.

Whether operated in-house or procured as a service, data centres are deeply embedded in modern industrial value chains and play an essential role in supporting the competitiveness of Europe's industrial base. However, they also raise questions regarding decarbonisation, as they account for around 1.5 per cent of total annual global electricity consumption[5]. This proportion could double by

[5] https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive/energy-performance-data-centres_en?utm

2030, mainly due to artificial intelligence. Also, supporting sustainability features for future data centres is key.

We call for a stronger recognition of sustainability within the DCAZ and DCSP mechanisms. In the Commission's proposal (Article 10), Member States only need to take into account environmental parameters when designating a DCAZ. For the Data Centre Strategic Projects (Article 14), it mentions "sustainable and innovative features" as one of the five possible criteria to get the label, and it can be bypassed, as data centres only need to meet two of them.

For both mechanisms, we propose using the upcoming regulation on minimum environmental performance standards for data centres. However, this future regulation will also need to make a clear distinction between new data centres and renovated data centres. It is not technically possible to have the same environmental expectations for both, and it is important to bear in mind that renovating a data centre avoids the carbon emissions embedded in the construction of a new one.

The EU minimum environmental performance standards for data centres that will be used by CADA are still under consultation. They should set achievable KPIs that reflect local and operational conditions. Relevant factors include, but are not limited to climate, water stress and the PUE/WUE trade-off; all renewable procurement routes, including on-site generation, PPAs and guarantees of origin; the feasibility of heat reuse; and each facility's IT load, age and design. Connect Europe and GSMA set out these points in more detail in their soon-to-be released joint response to the consultation.

Having a clear framework that supports sustainable data centre development would provide greater certainty for investors and support long-term decarbonisation.

Connect Europe key request

1. *Give greater weight to sustainability when designating Data Centre Acceleration Zones and selecting Data Centre Strategic Projects, based on achievable, contextualised KPIs and distinguish between new and renovated data centres.*