



*This European Parliamentary Research Service paper aims to inform Members on issues related to a forthcoming Commission initiative. It highlights the main choices which may shape the initiative and which Members may wish to explore ahead of formal Commission adoption. Based on documentary and other sources, it reflects the information available at the time of writing.*

*For further information on this topic, Members and staff of the European Parliament may contact: Tristan Marcelin, EPRS.*

# Cloud and AI development act

## ISSUES AT STAKE

**Data centres are key to innovation in artificial intelligence (AI).** Data centres are needed to access on-demand and scalable computational power and to deploy centralised digital services. Both are key in the lifecycle of large AI models, as their training and execution are intensive and centralised. Increased EU data centre capacity would benefit AI innovation, as would research and innovation to achieve resource optimisation and the decentralisation of computational tasks. Weak EU AI development could further hurt EU competitiveness across industries by slowing digitalisation.

**Data centre capacity in the European Union is insufficient.** The lack of capacity negatively impacts EU innovation, hindering economic growth. Studies suggest that despite comparable GDP, the United States has twice Europe's share of global data centre capabilities, and just three US-based companies account for 65 % of the EU cloud services market, which relies on data centres. Excessive dependence on non-EU capacity threatens the competitiveness of EU companies. EU data centre capacity-building is also hindered by legal and financial obstacles, as well as a lack of resources.

**EU-based secure cloud and AI computing services are lacking for highly critical use cases.** The EU's need for a sovereign digital transition is increasingly salient in the face of geopolitical shifts and growing global competition for innovation. Providers and customers lack legal clarity however, hindering enhanced availability and the use of EU-based highly secure cloud and AI offers. Member States did not manage to reach agreement in recent efforts to define the requirements for a sovereign cloud through a proposed European cybersecurity certification scheme for cloud services (EUCCS).



## An initiative for cloud and AI development

### Cloud computing and services

The European Union Agency for Cybersecurity ([ENISA](#)) defines **cloud computing** as the 'paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand'.

**Cloud services** are capabilities offered to customers via cloud computing. ENISA classifies cloud services by the type of underlying cloud capability.

1. **Infrastructure:** customers can directly use processing, storage or networking resources from the cloud service provider.
2. **Platform:** customers can use available development tools to deploy, manage and run their own applications in the cloud.
3. **Application:** customers can use applications available in the cloud, such as office software and file managers.

### AI lifecycle and cloud

The **lifecycle of an AI model** comprises several phases, including design, training, fine-tuning and deployment. The need for computational power depends on the model and its purpose. Simple AI models might not require a cloud infrastructure, while large models are likely to need one.

A large-language model (LLM) requires a large dataset of texts and a high-performance computer (HPC) for its training, but not for the execution of the model, known as inference. An LLM infers on servers scaled for its size, the number of requests, and other linked processes.

A cloud provides companies with on-demand and scalable computational capacity to train and deploy their AI models, as well as other digital services. Without the cloud, companies would need to invest and maintain their own infrastructure, which comes at a high cost.

### Edge computing

Cloud-based training and cloud-based deployment are common in the AI lifecycle. Providers can decentralise this computation on smaller devices placed on the edge of a given network, known as edge devices. For instance, instead of running large AI models in powerful data centres, providers could run optimised AI models directly on users' computers.

To drive long-term growth in the EU and raise living standards, in 2024 [Mario Draghi](#) spelled out the need to reduce the EU's dependencies while increasing competitiveness, including through computing and AI initiatives. Although researchers share the same view, [debate](#) is open as to how to achieve economic growth through digital means. The same year, the President of the European Commission [tasked](#) the new Executive Vice-President for Tech Sovereignty, Security and Democracy Henna Virkkunen with developing an EU cloud and AI development act (CADA) and a single EU-wide cloud policy for public administrations and public procurement, as recommended by

Draghi. According to the [Commission](#), the latter will complement the CADA to foster growth in European cloud providers and to support the use of highly secure cloud capacity.

The planned CADA is part of a broader set of initiatives to help the EU become a global leader in AI. The [AI continent action plan](#) succeeds the [AI Act](#) and structures the EU [strategy](#) for AI development and application, mentioning the CADA alongside [AI factories](#) and [AI gigafactories](#). While the latter two initiatives aim at providing ready to use high-performance computers (HPC) to train current and future AI models, the CADA focuses on creating the right conditions to improve EU cloud capacity.

The CADA would however not be the first EU legal act to set requirements on cloud markets. The [Data Act](#), most provisions of which have applied since 12 September 2025, laid down rules for cloud services providers, including requirements to ensure customers can easily switch between different providers. It also set safeguards against unlawful international transfers of non-personal data. The CADA would complement the Data Act by creating the right administrative conditions for a more vibrant European cloud and AI market, on top of existing obligations.

The Commission opened a [public consultation](#) for the CADA initiative, which ran from April to July 2025. The document provided by the Commission for the consultation stresses the need for a CADA based on the [objectives](#) of Europe's [Digital decade 2030 programme](#) (e.g. 75 % of EU companies should use cloud services with edge devices for their activities by 2030). The document hints at three distinct pillars where EU action would be needed: (1) advancing research and innovation, (2) creating the right conditions for investment in and deployment of data centres, and (3) ensuring highly secure EU-based cloud and AI computing capacity.

## First pillar: Advancing research and innovation

The first pillar aims to boost cutting-edge research and innovation in AI-enabling technologies and infrastructures. Given the time frame for research programmes, this pillar is likely to produce tangible results in the long term. Similar to the first pillar of the [EU Chips Act](#), the [chips for Europe initiative](#), it provides EU funding for research and innovation activities.

## Optimising resources for data processing

The development of advanced AI models requires a very large number of resources, notably energy. As the [Economist](#) reports, the International Energy Agency predicts that in 2026, data centres will globally need twice the energy they required in 2022 (reaching more than 800 Terawatt hours). As Draghi notes, the cost of energy in Europe is higher than in China and the US. Yet, access to energy remains key for the race to AI.

In the document accompanying the consultation, the Commission suggests leveraging 'research and innovation to make the EU a leader in **resource-efficient data processing infrastructure**'. [Experts](#) exploring this idea in 2024 indicate several technical solutions that could ultimately create an 'energy-aware data centre ecosystem'. The solutions include designing specific hardware for AI, optimising computation and deploying dynamic power-management systems.

Stakeholders are concerned by potential regulation overlaps. In their answer to the CADA public consultation, [Google](#) and [Deutsche Telekom](#) asked the Commission to maintain consistency with the [Energy Efficiency Directive](#), which comprises data centre monitoring and reporting obligations.

## Decentralisation and computation continuum

In addition to optimising resources for infrastructure, the Commission proposes a **computation continuum** as another means to securing AI leadership. A [computation continuum](#) is the integration of intermediate layers to address cloud limitations, including latency and cost. Concretely, instead of relying on one centralised workload in data centres, suitable computational tasks are shared among data centres, intermediate servers and edge devices, forming decentralised environments. The impact on the net sustainability of data processing can be positive.

## Chips for Europe initiative

At this stage, the Commission has not provided details of the ways it proposes to support research and innovation. However, the aim is comparable to the research and innovation pillar of the Chips Act, for which the [European Court of Auditors](#) forecast in 2025 that the policy will not reach its target of a 20 % share in the global market value chain by revenue. The court recommends an urgent reality check, as investment is insufficient. Its success depends on Member States' action, private sector investment, and external factors such as energy costs. The Commission's actions are limited. As for the CADA, creating the right conditions for investment falls under a separate pillar.

## Second pillar: Creating the right conditions for investment in and deployment of data centres

[McKinsey](#) notes that despite comparable GDP levels, the US has twice Europe's share of global data centre capabilities. It adds that in most cases, European data centres are owned by American tech companies (known as hyperscalers). The gap in computational capacity can be explained by fragmented and often lengthy permitting processes across EU Member States, the lack of specialised private players in Europe, and high energy costs. [Boston Consulting Group](#) (BCG) forecasts that hyperscalers will generate around 60 % of global data centre growth from 2023 to 2028. As Draghi notes, three hyperscalers currently account for 65 % of the EU cloud computing market, which relies on the data centre market. However, BCG adds that hyperscalers would rely on companies renting data centre sites to tenants, known as colocation providers, to meet the growing needs. Such tenants typically provide their own hardware.

To bridge the gap, the CADA's second pillar aims at creating the right conditions for attracting and supporting investment in sustainable data centres across the EU. The objective is to triple the EU's data centre capacity within the next five to seven years.

## Obstacles in Europe for investment in data centres

The Commission notes that **difficulties in accessing water and energy** in the EU hinder investment in data centres, impacting the EU data centre sector negatively. In addition, **difficulties in accessing land** have also been identified as hindering investment. The Centre on European Regulation ([CERRE](#)) notes the process to obtain a permit to build data centres is not harmonised across Member States. Lastly, the Commission indicates the process of developing data centres is highly capital-intensive, creating **capital barriers** for the entry of new players to the market. In comparison, BCG believe that hyperscalers will need to spend around US\$1.8 trillion in data centre-related capital expenditure from 2024 to 2030 to match the surging demand in the US.

## Creating the right conditions for investors

Regarding access to energy, CERRE suggests enhancing energy flexibility through **strategic grid user integration**. For land permits, they suggest harmonising the process among Member States and creating a **fast-track process** for projects with social impact. In its answer to the CADA public consultation, [Microsoft](#) mentions the Aragon region in Spain as having a successful single streamlined permitting process with a fast-track procedure for strategic projects.

To provide the **capital to help new players** access the market, [experts](#) recommend using the proposed new [European competitiveness fund](#) (ECF) alongside EU rules laying down a strategy, and public and private investment to support critical technology innovators. The ECF would aim to consolidate 14 EU funding instruments in one framework. The [Finnish](#) government notes action is needed to ensure 'the benefits of building data centre capacity do not primarily flow to actors outside the EU'. Defining and supporting EU-based cloud and AI computing capacity is the third CADA pillar.

## Third pillar: Ensuring highly secure EU-based cloud and AI computing capacity

European technological sovereignty, including cloud sovereignty, increasingly features on the EU political agenda. In October 2025, the European Council's [conclusions](#) advocated a sovereign digital transition and asked the Commission to be ambitious in its proposal for an EU cloud and AI development act. At the same time, an Industry, Research and Energy (ITRE) Committee [report](#) on European technological sovereignty and digital infrastructure within an own-initiative procedure is awaiting a [final vote](#) in the European Parliament. The report notes geopolitical shifts and technological competition.

The third pillar of the CADA focuses on ensuring that 'a set of narrowly defined highly critical use cases can be operated using highly secure EU-based cloud capacity' and on creating the conditions for the EU cloud industry to develop such an offer. Stakeholders mentioned [defence](#) programmes, [public administration](#) and critical infrastructure as relevant use cases.

## Defining a highly secure EU-based cloud capacity

Defining the requirements for highly secure EU-based computing capacity is the key [challenge](#). The ITRE committee report notes that previous EU discussions on this matter, with the proposal for a cybersecurity certification scheme for cloud services (EUCS), 'have not brought any results'. The [EU Institute for Security Studies](#) (EUISS) explains that divergences between Member States block the scheme's adoption and delay progress on other initiatives.

As an example definition of highly secure cloud capacity, the US relies on the [Federal Risk and Authorization Management Program](#) to standardise cloud services used by federal agencies for secure uses. Companies are authorised to sell services with high impact to the federal government if they comply with requirements including encryption standards, incident response, personal and physical security and risk management. More recently, the Commission published a [cloud sovereignty framework](#) linked to its recent [competition](#) to procure sovereign cloud services over six years for EU institutions, bodies, offices and agencies. The framework details several assurance levels for each defined objective, the maximum level being where the technology and operations are

**under complete EU control and only subject to EU law.** [Dassault Systèmes](#), a French software company, suggests one requirement for defining sovereignty is that cloud providers should be headquartered within the EU. Conversely, hyperscaler [representatives](#) encourage an open market with no such requirement. German software company [SAP](#) argues that such new rules are unnecessary, as existing EU-certified infrastructure, such as under the EUCS, are sufficient.

## Providing the right conditions for an EU cloud industry

The EUISS notes that non-European cloud providers have developed sovereign regional cloud solutions which could comply with several sovereignty requirements. However, it would not fully eliminate the risk of external interference. The Draghi report calls solutions where the infrastructure is not fully European 'Europe's second-best available option today for data security and territorial sovereignty'. As an example, the Italian public administration's cloud [strategy](#) authorises the use of hybrid cloud services for the maximum level of criticality. Hyperscalers can provide services, but encryption and operational requirements apply.

[Sopra Steria](#), a French company specialised in digital solutions, as well as [France and Germany](#) recommend **using public procurement** to drive the emergence of competitive and trustworthy EU solutions. At the same time, [Microsoft](#) called for the EU to avoid measures that would discriminate against non-EU actors, going against EU commitments under the World Trade Organization Agreement on Government Procurement. The Court of Justice of the EU ruled in 2022 on a [case](#) related to the tender of a HPC suggesting an EU institutional public procurement procedure can include an 'EU added value' criterion. However, clearer EU regulatory guidance, beyond HPC procurement, could enhance the availability and use of EU-based highly secure cloud and AI offers.

## MAIN REFERENCES

European Commission, [Call for evidence for an impact assessment for the Cloud and AI development Act](#), March 2025.

Draghi, M., [The future of European competitiveness – A competitiveness strategy for Europe](#), September 2024.

## DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2025.

[eprs@ep.europa.eu](mailto:eprs@ep.europa.eu) (contact)

<https://eprs.in.ep.europa.eu> (intranet)

[www.europarl.europa.eu/thinktank](http://www.europarl.europa.eu/thinktank) (internet)

<http://epthinktank.eu> (blog)