amazon

Introduction

Amazon welcomes the opportunity to contribute to the Call for Evidence and Public Consultation (collectively, "the Consultation") on the future EU Cloud and AI Development Act ("CAIDA") and to provide our views on the questions and proposals outlined by the Commission.

Amazon is committed to Europe, with deep investment and partnership going back more than 25 years. Since 2010, Amazon has invested over €320 billion in Europe, including more than €225 billion in the EU alone, and employs more than 230,000 people (including over 150,000 in the EU). **These investments, including tens of billions of euros in cloud infrastructure across several EU countries** - including France, Germany, Italy and Spain - **underscore long-term commitment** and belief in Europe's potential. We opened the first Amazon Web Services (AWS) Region[1] in 2008 in Dublin and **today operate eight AWS Regions across Europe (six of them in the EU), with infrastructure in more than 20 countries, including 120+ CDN (Content Delivery Network) points of presence across 19 EU countries**.

We help enable Europe's growth and competitiveness objectives by providing European organizations of all sizes with access to cutting-edge technologies, most notably in artificial intelligence. From innovative startups like Mistral AI and Poolside to industry giants such as Siemens and BMW, European companies are leveraging AWS to achieve extraordinary results, compete globally, and drive innovation right here in Europe. The success driver for this broad adoption of AWS services is our focus on **democratizing access to AI**. Through services like Amazon Bedrock, we are making foundation AI models easily accessible, allowing businesses to experiment and innovate at every stage of development, and scale flexibly at usage-based costs. Customers can choose between different AI models and change cloud providers easily. Our investment in custom AI chips like AWS Trainium and Inferentia further drives down costs and expands access to the compute power necessary for AI innovation. We are committed to working with policymakers to ensure competition in AI thrives and that the benefits of this technology are widespread.

Lastly, AWS is building a **sustainable cloud infrastructure** to help customers achieve their sustainability goals while maintaining the security, performance, reliability, and cost-efficiency they expect. As part of Amazon's commitment to reach net-zero carbon by 2040 through The Climate Pledge, AWS continually innovates to improve efficiency and reduce environmental impact across our global infrastructure.

We therefore commend the European Commission's goal to increase the availability of sustainable compute capacity in the EU by **removing current blockers to accelerate data center investments and deployment**, ranging from **facilitating access to natural resources** to **streamlining burdensome permitting procedures**. We also welcome the goal that the Commission sets out as regards ensuring there is a sufficient **pool of EU-based highly secure cloud services to serve highly critical use cases in Europe**, if **criteria for services that meet this high bar are non-discriminatory and based on technical and organizational requirements and controls.**

[1] AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. We call each group of logical data centers an Availability Zone (AZ). Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZs to achieve even greater fault-tolerance.

As a company with a broad infrastructure footprint across Europe and years of experience in serving customers in critical sectors (from critical infrastructure operators to national security and defense institutions), we believe we bring a strong contribution to the Commission's efforts to define technical and organizational standards for the security and sovereignty of critical data.

In doing so, we do however want to **caution against introducing new regulatory obligations for cybersecurity and resiliency** to either **cloud providers or cloud customers in critical sectors.** First, it should be analyzed how **existing rules in the broad regulatory framework that has recently been adopted can be leveraged to achieve security and resilience goals.** Risk management and operational resiliency requirements have been introduced for organizations operating in critical sectors (including digital service providers) through regulations that recently came into force and have yet to deliver on their objectives (**DORA, Data Act, NIS2, Cyber Resilience Act, Critical Entities Resilience Directive**) – and for which companies are rolling out resource intensive compliance programs. We recommend **allowing sufficient time for implementation, assessing the impact of existing regulations and only then considering what gaps remain to be filled and if regulatory intervention is necessary** or whether guidelines (e.g. in the form of cloud procurement guidelines for public sector organizations) would be a more appropriate way to achieve those goals.
Introducing new regulatory requirements only after the impact of comparable or overlapping existing regulations has been evaluated would also **align with the Commission's initiative to simplify EU digital regulations.** This is also true when it comes to addressing competition concerns related to the Cloud and AI services, where we believe the current regulatory framework is already fit for purpose to address potential concerns and where competition is working well.

1. Simplify data center development across the deployment and operation cycles

Developing data centers requires a complex due diligence process to assess where there is suitable land that allows for data center development, available resources such as power, water and fiber, an understanding of permitting processes and available workforce. Significant resources are required to identify locations. Once a location is identified, it takes several years before operations can begin due to complex permitting. The next challenge is scaling operations, as data centers continue to ramp and expand as customer demand grows. Looking at the entire development and operation cycle, there are opportunities to simplify and speed up some of the existing processes across site selection, grid connection and permitting.

We welcome policies that support data center development and help meet Europe's growing technology needs. These should focus on simplifying all aspects of data center development: site selection, deployment and scaling. They should be non-discriminatory and available to all operators based on objective criteria. From our perspective there are three areas that should be the focus in the Cloud and AI Development Act:

1) Improve access to information to speed up site selection
2) Streamline and simplify grid connections
3) Introduce fast-track permitting for datacenters

Improve access to information to speed up site selection
Suitable locations are zoned for industrial and/or data center development, close to utility networks (water and electricity), have robust connectivity networks and available skilled workforce. Data center operators strive to locate in as beneficial locations as possible, where minimal additional infrastructure is

needed to be built while also factoring in latency requirements for customers using the services within the data center.

Recommendation: Increase the availability of and access to information necessary for data center developers to speed up site selection by: i) identifying areas of available brownfield sites and greenfield sites zoned for industrial use; ii) mapping available power, water, and fiber and making this information available to data center developers; and iii) making investment agencies in Member States responsible for collecting and sharing this information with data center developers.

Streamline and simplify grid connections

Securing a grid connection is another major bottleneck for data centers and economic growth. Alongside the growing digital sector and AI, the energy sector is undergoing massive transformation with rapid electrification of transportation and heating, and an increase of renewables in the energy mix. To ensure success across industries, grid infrastructure investments must keep pace with demand growth. On the ground, businesses are increasingly experiencing connection delays and uncertainty around when capacity will become available. This makes it incredibly difficult for businesses to plan and execute their growth strategies, including building AI Infrastructure.

Recommendation: To ensure that European grids can grow at the pace needed, focus on: i) enabling proactive grid investment based on future growth projections; ii) addressing energy infrastructure permitting to speed up grid reinforcements by introducing a fast-track process for strategically important power lines; iii) making the grid connection process more efficient and ensuring that real projects, rather than speculative ones, are prioritized given the large increase in applications; and iv) attract flexibility measures through market-based incentives. Compass Lexecon recently released a report that explores successful market designs and regulatory support schemes to foster the deployment of low-carbon flexible assets.

Introduce fast-track permitting for datacenters

For secured sites, several permits are required to construct and operate data centers, such as building and environmental permits. Many require a lengthy and complex process with different authorities at different stages and may or may not be able to run in parallel. These also vary from country to country, and sometimes within the country between regions. To facilitate data center development, a fast-track simplification scheme should be introduced to streamline the permitting process. Based on our experience, the PIGA-process in Aragon, Spain, has been successful to reduce the administrative burden on companies and most importantly the handling time, while ensuring a high compliance standard with applicable regulations. Another example is Italy and its simplified administrative procedure to promote strategic foreign investments in infrastructure.

Recommendation: Introduce fast-track procedures for data center projects that meet defined criteria to improve the relevant administrative processes for the benefit of data center developers, government bodies and authorities involved. This would include: i) Establishing a clear and structured application process for such a fast-track procedure and clarifying how the thresholds for application apply, e.g. minimum level of investment needed; ii) Appointing a single authority for the data center developer to engage with during the permitting process with a dedicated permit liaison in other competent authorities; iii) Removing procedural dependencies to allow for parallel processing of permits; iv) Establishing a clear framework for the fast-track procedure to include clear timelines/maximum handling timelines and clear information and documentation requirements; and iv) Clarifying the rules related to the scope of appeals and standing.

2. Promote sustainable data center development

AWS seeks to operate as efficient and sustainable data centers as possible. We continuously innovate our infrastructure design, build, and operations to make progress towards net-zero carbon by 2040 and being water positive by 2030. As there are already several policy and legislative frameworks currently being developed on this, we advocate for a unified regulatory approach to sustainable data center development.

Rely on the data center rating scheme developed by DG ENER

AWS recognizes that the EU's vision to introduce a new energy efficiency policy framework for data centers represents an opportunity to drive greater transparency and environmental accountability across the sector. It will enable customers, operators, and investors to make informed decisions while identifying areas for performance improvement. Hence, to achieve these goals, the framework must be built around measurable KPIs across the data center industry, must seek to incentivize efficient use of data center infrastructure and must foster technical innovation under the principle of technological neutrality. The scheme must also account for the diverse operational requirements and characteristics of different data centers, while rewarding organizations that invest in innovative solutions to accelerate Europe's path to climate neutrality.

Recommendation: DG ENER is already working on a comprehensive Energy Efficiency Package for data centers, and we strongly recommend against introducing parallel criteria in the Cloud and AI Development Act that could create regulatory overlap and potential conflicts. Premature implementation risks cementing flawed metrics into long-term policy and creating market distortions that could undermine the EU's broader digital and AI ambitions.

A phased, evidence-based approach to the upcoming Data Centre Rating Scheme is essential. We propose that implementation begins with a self-improvement system from May 2027 and evolves into a comparative system by 2030, once sufficient market data and operational experience have been gathered. This measured approach allows for the refinement of metrics and methodologies based on real-world implementation. A scoring mechanism which evaluates data centers holistically through a point-based system should be used. This would consider core sustainability pillars while acknowledging operational trade-offs. It would encompass energy efficiency, water consumption, and IT performance, complemented by transparent disclosure of additional sustainability initiatives. Such an approach provides a more nuanced and complete picture of a data center's environmental impact.

The introduction of minimum performance standards at this stage would be premature and counterproductive. Complex trade-offs between energy efficiency, water consumption, and heat reuse potential make rigid performance standards unsuitable without comprehensive market understanding. Moreover, such standards could compromise the very goals they aim to support - sustainability, innovation, and digital resilience. We recommend building on the valuable insights gained from Energy Efficiency Directive reporting to refine metrics before expanding requirements to other regulatory frameworks. This evidence-based approach ensures effective and future-proof policy making while maintaining the EU's competitive edge in digital infrastructure development.

Enable industrial water reuse through the EU Water Resilience Strategy

As the demand for digital infrastructure grows, so does the need for sustainable water management in the data center industry. Modern data centers employ various cooling technologies, including evaporative cooling systems, to achieve water efficiency while maintaining thermal performance. It is essential to

consider data center water usage within the broader context of industrial consumption. Water conservation gains can be amplified through access to alternative water sources, particularly industrial water reuse. Treating and reusing municipal wastewater for non-potable applications such as industrial cooling, urban landscaping, and environmental restoration significantly reduces demand for freshwater sources. Higher-quality freshwater resources are reserved for drinking water and food production.

Recommendation: To avoid duplication and diverging regulation, we recommend that water topics are addressed in the upcoming EU Water Resilience Strategy, to: i) ensure a cross-sectoral approach, with water management policies reflecting the broader industrial landscape rather than singling out specific sectors like the data center sector; ii) create enabling conditions for EU-wide industrial water reuse and iii) focus on closing gaps in water management without duplicating requirements.

3. **Focus on technical and organizational measures that ensure data security and sovereignty for highly critical use cases within the existing legal framework**

According to the call for evidence, the CAIDA will seek to tackle 'the lack of a competitive EU-based offer of cloud computing services at sufficient scale to serve highly critical use cases with particularly high security needs, as found in various economic sectors and the public sector'.

At AWS, we have developed deep expertise in supporting customers across the public sector, critical infrastructure sectors, and defense by providing secure, scalable, and resilient cloud services tailored to highly sensitive workloads. Globally, AWS enables government agencies, healthcare providers, energy companies, and defense organizations to modernize their IT infrastructure while ensuring compliance with stringent regulatory and security requirements, underpinned by a resilient infrastructure. For highly sensitive workloads across the world, we have built specialized regions, end-to-end encryption, granular access controls, and robust identity and threat management solutions. These capabilities help organizations safeguard classified or mission-critical data against cyber threats, maintain operational resilience, and accelerate secure digital transformation. AWS's compliance with international and national security standards and qualifications, including ISO 27001, FedRAMP, C5 (Germany) and Italy's QC2 qualification to host critical data and workloads further reinforces our position as a trusted partner for handling the most sensitive and high-impact workloads across sectors.

In our commitment to offer customers the most advanced set of sovereignty controls and features available in the cloud, we are continuously investing in technical capabilities for:

(1) **Control over data location**: currently in the EU, customers have the choice to deploy their data into any of the six existing Regions.

(2) **Verifiable control over data access**: we have designed and delivered first-of-a-kind innovation to restrict access to customer data. The AWS Nitro System, which is the foundation of AWS computing services, uses specialized hardware and software to protect data from outside access during processing on Amazon Elastic Compute Cloud (Amazon EC2). By providing a strong physical and logical security boundary, Nitro is designed to enforce restrictions so that nobody, including anyone in AWS, can access customer workloads on EC2.

(3) **The ability to encrypt everything everywhere**: currently, we give customers features and controls to encrypt data, whether in transit, at rest, or in memory. All AWS services already support encryption, with most also supporting **encryption with customer managed keys that are inaccessible to AWS**. We commit to continue to innovate and invest in additional controls for sovereignty and encryption features so that our customers can encrypt everything everywhere with encryption keys managed inside or outside the AWS Cloud.

(4) **The resilience of the cloud**: It is not possible to achieve digital sovereignty without resiliency and survivability. **Control over workloads and high availability** are essential in the case of events like supply chain disruption, network interruption, and natural disaster. Each AWS Region is comprised of multiple Availability Zones (AZs), which are fully isolated infrastructure partitions. To better isolate issues and achieve high availability, customers can partition applications across multiple AZs in the same AWS Region. For customers that are running workloads on premises or in intermittently connected or remote use cases, we offer services that provide specific capabilities for offline data and remote compute and storage. We commit to continue to enhance our range of sovereign and resilient options, allowing customers to sustain operations through disruption or disconnection.

In Europe, we went one step further and announced a new, independent cloud infrastructure designed specifically for Europe, to launch by the end of 2025. The AWS European Sovereign Cloud was designed to meet the evolving digital sovereignty needs of European customers in the public sector and in highly regulated industries. **Located and operated within Europe, the AWS European Sovereign Cloud will be physically and logically separate from existing AWS Regions.** AWS will establish a new European organization and operating model for the AWS European Sovereign Cloud, with a new parent company and three subsidiaries incorporated in Germany. These dedicated European subsidiaries will **1/implement controls for keeping customer content and customer-created metadata within the EU**, **2/employ EU resident personnel responsible for operating the AWS European Sovereign Cloud**, **3/own and operate the underlying infrastructure, and hold EU-based root certificates and trust services that are needed to authenticate the security and identity of cloud services**. The management team leading this new parent company will include the managing director and a government security and privacy official, **all EU citizens residing in the EU**. AWS will establish an **independent advisory board for the AWS European Sovereign Cloud**, legally obligated to act in the best interest of the AWS European Sovereign Cloud. The advisory board will act as a source of expertise and provide accountability on sovereignty-related aspects of the AWS European Sovereign Cloud operations, including strong security and access controls and the ability to operate independently in the event of disruption.

Building on deep experience running AWS services for the most sensitive workloads around the world, the AWS European Sovereign Cloud is designed with the operational resilience our customers expect from AWS. The design of the AWS European Sovereign Cloud enables it to **continue operations even in the event of a connectivity interruption between the AWS European Sovereign Cloud and the rest of the world**. European customers and governments benefit from the resilient AWS architecture that features multiple Availability Zones with independent power, networking, facilities, and security capabilities that make these critical operations possible. This powerful combination has proven crucial during times of crisis, such as helping to preserve vital Ukrainian government services and developing AI-powered early warning systems for flood prevention in Zaragoza - demonstrating how AWS enables meaningful support when Europe needs it most. The AWS European Sovereign Cloud will feature the same architecture that has proven crucial at critical times, enabling continuous operation in the event of a natural disaster. To support continuity even under extreme circumstances, authorized AWS employees of the AWS European Sovereign Cloud, who are EU residents, will have independent access to a replica of the source code needed to maintain the AWS European Sovereign Cloud services.

We have developed the European Sovereign Cloud to ensure that our customers, whether in highly regulated or critical sectors such as Government and National Security and Defense, maintain their ability to choose highly secure and innovative technologies that enable them to effectively achieve their mission without compromising on sovereignty.

To satisfy customer requirements for the AWS European Sovereign Cloud, we are introducing the Sovereign Requirements Framework (SRF). The SRF is a comprehensive set of technical, legal, and operational sovereignty controls that were developed from the sovereignty expectations of our customers, requirements of regulatory bodies across the EU, industry-leading framework guidance, and the needs of our implementation partners. With the SRF, AWS will demonstrate adherence to sovereignty expectations and enable verifiable trust in a consistent and repeatable manner to customers and regulators through control implementation across services and operations creating auditable evidence. From launch, AWS commits to independent third-party audits and attestations of the AWS European Sovereign Cloud controls based on the SRF and will be included in the AWS European Sovereign Cloud specific SOC2 attestation. The comprehensive sovereignty controls framework encompasses multiple layers of protection designed to ensure **operational autonomy** and **data sovereignty** within the defined partition. This includes robust **business continuity measures for independent operations**, strict **data isolation and encryption protocols**, **EU-based governance of all customer contracts and dispute resolution**, **rigorous access controls limited to EU-resident personnel**, and **hardened physical security measures**. All systems, from infrastructure to personnel management, are designed to maintain operational independence while **ensuring that customer data remains within EU jurisdiction and under EU law**, with all **critical operations and decision-making occurring within the defined sovereign boundary**. This multi-layered approach creates a fully autonomous environment where **data handling, system management, and legal oversight are firmly rooted within European territory and control**.

Recommendations:

- **Adopt an approach to security and sovereignty requirements for critical use cases that is grounded in technical and organizational controls** which provide **strong assurances in terms of customer control over data and operational resilience,** without being overly prescriptive. We **caution against criteria based on company ownership or global headquarters** and we believe such criteria do not translate into increased security, resiliency and ultimately sovereignty for public administrations or for highly critical use cases. Reliance on a diversified global supply chain is often more robust in times of crisis. Moreover, in today's global digital economy, companies are most often subject to multiple jurisdictions, making their ownership structure less relevant than their implemented safeguards. We also believe that preserving customer choice is critical if Europe is to advance its competitiveness goals and digital decade targets.

- **Encourage partnerships across the industry, without being overly prescriptive**. The Draghi Report presented a pragmatic vision for cloud policy in Europe, combining robust sovereignty controls with existing world-class cloud capabilities. Specifically, the Report recommends collaboration between EU and non-EU CSPs to develop a competitive domestic industry for sovereign cloud solutions. This aligns perfectly with AWS's approach. Through our EU Regions, we enable European organizations to access world-class cloud capabilities while maintaining full control over their data and we demonstrate this further through partnerships with European industry leaders like Thales, Eviden and T-Systems, who manage and control encryption keys outside of the AWS environment through AWS External Key Store. Partnerships should be encouraged in a way that allows companies to come together in the ways that are most suited to their business models and strengths, avoiding a one-size-fits-all approach that may not be economically viable (e.g. asking companies to form joint-ventures).

4. **Take stock of existing regulations meant to mitigate cybersecurity, resiliency and data protection risks, as well as other risks identified in the consultation, such as vendor lock-in**

Cloud service providers are already subject to **security requirements** and **direct oversight** under NIS2 and, for those designated as critical providers, under DORA. **Customers in critical sectors are also already covered by robust cybersecurity and resilience frameworks such as DORA, NIS2, CER, and the CRA**. These frameworks **mandate that they apply thorough risks management and business continuity processes**, which imply assessing all types of risks to their critical data, including supply chain risks, and adopting appropriate mitigation measures. Organizations are best positioned to classify their data, assess risks (including likelihood and impact) based on their unique context—size, structure, technology stack, and risk appetite—and determine appropriate safeguards. We therefore caution against introducing new requirements that would seek to prescribe how companies should assess and mitigate against individual risks and instead allowing them flexibility in their risk management approaches.

The robust regulatory framework for cybersecurity, resiliency and data protection adopted in recent years has also created new obligations for national and European authorities – we recommend allowing time for these authorities to implement their new responsibilities before adding new ones. For example, Critical Third-Party Providers (CTPPs) under DORA will be subject to continuous oversight by EU financial supervisors. Imposing additional requirements or restrictions on this sector could overlap or even conflict with the mandate given to EU financial regulators and the overall risk management and operational resiliency framework included in the Regulation.

Regarding concerns about specific risks such as the extraterritorial reach of non-EU laws like the U.S. CLOUD Act, it is essential to provide European users with more clarity as regards its applicability, as well as factual data about its impact. In our view, the CLOUD Act is often misunderstood. It does not give U.S. law enforcement unrestricted access to data. It makes available a mechanism through which law enforcement can go before a judge to request a service provider produce specific content that has a nexus to an alleged crime. The CLOUD Act also creates additional safeguards for cloud content, recognizing the right of cloud service providers to challenge requests that conflict with another country's laws or national interests, including GDPR.

Moreover, there are technical and organizational risk mitigation measures that customers can adopt to protect against it, including strong encryption, key management services and contractual protections, which AWS makes available to customers. Many of the AWS core systems and services are designed with zero operator access, meaning the services don't have any technical means for AWS operators to access customer data in response to a legal request. Historically, we have received very few United States law enforcement requests for customer content, and we are transparent about the number of requests that we receive. **There have been no content data requests to AWS that resulted in disclosure of enterprise or government data stored outside the U.S. to the U.S. government since AWS started reporting this statistic.**

The CLOUD Act applies to all electronic communication service or remote computing service providers that operate or have a legal presence in the U.S.—regardless of where their headquarters are located. For example, European-headquartered cloud providers with U.S. operations are equally subject to the Act's requirements. The requirements of the CLOUD Act are also consistent with laws of other countries. According to a 2024 filing by the U.S. DOJ, the laws of several European Union member states, including Belgium, Denmark, France, Ireland, and Spain, have similar requirements. In fact, since 2023, most law enforcement requests that AWS receives come from authorities outside of the United States. Additionally,

the EU's e-Evidence Regulation, 2023/1543, adopted in August 2023, authorizes Member States to "order a service provider […] to produce or preserve electronic evidence regardless of the location of data'.

The Data Act (which will become applicable from September 2025) already includes obligations for cloud service providers to implement **technical, organizational, and legal safeguards to prevent unlawful third-country access to non-personal data stored in the EU**. It outlines procedures for cases where third-country orders conflict with EU law and complements the GDPR's protections for personal data.

Furthermore, **the Data Act establishes important obligations designed to promote data portability and switching, interoperability, transparency and contractual clarity and support for data sharing and access**. These provisions are meant to reduce vendor lock-in, promote the use of multiple providers and facilitate switching, therefore effectively reducing over-reliance on a single provider and mitigating risks related to continuity of service.

Jointly, these regulations create a broad regulatory framework that can help mitigate most of the risks emphasized by the Commission in the public consultation questionnaire and call for evidence. **The Commission should first evaluate how providers comply with these requirements and whether any gaps can be addressed through effective enforcement before considering additional legislation**.

Recommendations:

- **Reduce regulatory burden and align CAIDA with the Commission's simplification agenda.** We urge the Commission to first take stock of the substantial body of existing regulations covering cybersecurity, data protection and operational resilience for both cloud service providers and cloud customers and determine whether the security objectives in CAIDA can be achieved through proper implementation and enforcement of existing rules, aided by softer measures such as recommendations and guidelines. These can help customers in their procurement and risk management processes and give providers a blueprint for what is considered a high bar in Europe in terms of security and sovereignty, thus enabling them to further invest and compete. In doing so, the Commission should seek to align with other initiatives under development (e.g. the European Cybersecurity Certification Scheme for Cloud Services) and avoid duplication.

- **Avoid prescriptive approaches and instead guide organizations in adopting a risk-based framework.** EU-wide Guidelines (e.g. such as the ones developed by ENISA for NIS2) can help with the implementation of the above-mentioned controls in a harmonized way across the Single Market. However, customers remain the best placed to assess the criticality of their cloud workloads, the risks across their supply chain and to decide on the best risk mitigation approaches and how to select between the different providers and solutions on the market. The Commission should recognize this and empower cloud users instead of prescribing strict regulatory requirements.

5. Support uptake of cloud by public sector organizations in procurement

Cloud adoption (together with AI and data analytics) among European enterprises is falling short of the EU's 2030 Digital Decade targets. According to the European Commission's latest Digital Decade report, cloud adoption among businesses is projected at 64.4%, while AI uptake is only 16.8% (vs. the 75% target for each). Although no specific public sector targets exist for these technologies, related goals—such as

achieving 100% digital availability of key public services—highlight the **need for increased cloud uptake across public administrations to meet broader digital transformation and competitiveness objectives**.
However, public procurement of cloud services faces persistent challenges, from slow and rigid procurement processes that are not fit for purchasing cloud and AI services, to lack of in-house expertise. There is a need to invest in digital renewal of public services, to overhaul legacy systems and capitalize on the spin-off effects in the private sector.
Within European public procurement more broadly, the European Court of Auditors has identified a persistent lack of competition in tenders—a key concern that underpinned the most recent revision of the Procurement Directives. Any future revision of the Directives or related guidelines should begin with the goal of enhancing competition and openness in procurement processes.

Recommendations:

- Adopt Procurement guidelines for cloud that encourage **inclusive participation by a wide range of providers, irrespective of the geographical location of their global headquarters,** and allow public sector buyers to select services based on **fair, transparent, and objective criteria**. This will empower public administrations to adopt cloud solutions best suited to their needs and support their digital transformation agendas. Exceptions from EU procurement rules should remain narrowly defined and subject to clear, proportionate justifications. Loosening these rules risks undermining the integrity of the Single Market and could conflict with the EU's international obligations, including reciprocal market access commitments under agreements like the WTO Government Procurement Agreement (GPA).

- Where procurement preferences are introduced, they should not apply to entities from GPA contracting parties. In cases where preferences are based on national security exceptions, these should avoid geographic exclusions and instead rely on **objective, risk-based criteria**—such as operating under the rule of law, adherence to due diligence standards, and strong compliance track records. As the European Commission develops a common policy for cloud procurement in the public sector, it should consider risk mitigation strategies inspired by the 5G Toolbox, focusing on continuity and data protection without resorting to disproportionate restrictions.

6. In the AI space, competition is working well to deliver value and choice - regulatory intervention on aspects related to competition is unnecessary and might hinder innovation

The Consultation also poses questions on competition aspects of cloud and AI services. These concerns must be considered in the context of an **AI and cloud landscape marked by unprecedented innovation and growing competition across all levels of the value chain**[2]. Rather than inhibiting customer choice, the cloud has made switching between IT providers easier than ever before and has been a catalyst for the launch of innovative and diverse services. There is a large body of evidence demonstrating that this sector is characterized by a rapid pace of innovation, declining prices, and intense competition.

Still, data shows that less than 15% of IT spend globally is on cloud services, whereas approximately 70% of IT workloads are on-premises. This means there is much space for growth, and competition remains

[2] Refer to recent studies on this:
https://cerre.eu/wp-content/uploads/2025/07/What-policy-interventions-for-a-competitive-AI-sector_Final.pdf
https://www.rbbecon.com/publication/article/why-current-genai-market-dynamics-suggest-competition-is-working/

fierce from new entrants capitalizing on this opportunity, as well as from on-premises IT providers and private cloud providers. This high level of competition is evident from the declining prices in the sector (AWS has reduced prices at least 151 times since launch, and other providers have similarly reduced prices over time), high degree of innovation (just in the last year, AWS introduced 6 new services and thousands of new features), and significant investment.

Today, the AI industry is experiencing rapid development and intense competition at all levels—from foundation model development to computing infrastructure and applications. Major tech companies are racing to deliver AI services, while billions in venture capital are flowing into specialized cloud providers and startups developing novel AI models. This competitive dynamism is generating better value, service, and choice for enterprises and consumers alike.

AI development resources—such as compute power, talent, and infrastructure—are offered by a broader array of players, including traditional hardware vendors (e.g. Dell, who is partnering with Meta and Hugging Face or Hewlett Packard, who is launching a cloud service to train generative AI models), and specialized cloud providers focusing on AI training and inference like CoreWeave, LambdaLabs, G42, Crusoe, Cirrascale, TensorWave, and RunPod. This diversity shows that market forces are effectively expanding access and driving innovation.

On the foundation model front, competition is similarly robust. Alongside major providers like AWS, OpenAI, Google, Meta, and Microsoft, a vibrant ecosystem of startups is advancing both open-source and proprietary models—such as Mistral AI, Cohere, Hugging Face, Anthropic, and many others. Meanwhile, thousands of generative AI applications are being developed globally, with over 1,400 tracked by Dealroom and nearly half of surveyed companies customizing or building their own models, according to McKinsey. The Commission itself has acknowledged that in the future the leading models may be smaller and lower cost AI models[3], which suggests that it is not just AI developers with critical mass that can be competitive in the market, but rather that there is space for smaller AI developers and new entrants.

These developments, alongside the high level of investments in both AI and the cloud sector[4], underscore that competitive pressure is strong and, given the pace of change in AI development and foundation model related areas, intervention in this nascent and evolving space is unwarranted.

Concerns such as tying, bundling, or exclusive dealing fall well within the scope of existing antitrust tools. As competition authorities have acknowledged, most potential risks in this space are addressable under traditional doctrines. New laws or sector-specific regulation should only be considered where clear regulatory gaps exist and should be carefully calibrated to avoid stifling innovation or raising entry barriers for emerging players.

Moreover, as previously stated, EU legislation already directly addresses any potential lock-in and interoperability concerns identified (in our view incorrectly). The EU Data Act contains detailed **obligations for cloud service providers to facilitate customer switching and multi-provider use.** It mandates the **removal of technical, contractual, and commercial obstacles to portability** and includes specific rules prohibiting obstacles inhibiting customers from **unbundling "infrastructural elements" from other cloud services**, enabling customers to decouple and transition services more easily.

[3] https://competition-policy.ec.europa.eu/document/download/c86d461f-062e-4dde-a662-15228d6ca385_en
[4] https://www.rbbecon.com/publication/article/why-current-genai-market-dynamics-suggest-competition-is-working/

We are committed to working closely with the Commission on interoperability and other implementation aspects of the Data Act, to ensure it works well for customers and providers. AWS does not impose technical barriers that prevent customers from switching or multi-clouding. We attract and retain customers by building our services to industry-leading standards of security, availability, durability, and by offering interoperability with third-party services or applications. We have therefore invested heavily to ensure that customers can choose the IT services and technologies that best suit their needs, including the ability to switch providers and multi-cloud where desired. Our core services (i.e., compute, storage, database, analytics, and networking), which are the main services customers use, enable customers to build fully interoperable and transportable solutions, which are cloud agnostic. They all use open protocols, interfaces, application programming interfaces ("APIs"), and data formats, allowing customers to use the optimal technologies for their specific use-cases. In addition, we make a comprehensive suite of software development kits ("SDKs") available under open-source licenses, enabling anyone to write interoperable applications against our APIs, and actively contribute to several open-source projects that customers can use with Amazon EC2, thereby enhancing interoperability across different cloud environments.

Recommendation: **Leverage the existing tools to address competition concerns in cloud and AI and refrain from increasing the regulatory burden, which could inadvertently slow down adoption**.
While monitoring developments on the market is essential given the rapid pace of technological change, premature regulatory intervention risks disrupting healthy market competition and stifling innovation at this critical developmental stage. Regulatory enforcement should be reserved for cases where there is compelling evidence of actual harm. To secure the dynamism of the cloud and AI sectors, the simplification of data center development across the deployment and operation cycles as detailed above is essential as well as facilitating access to capital and simplifying the regulatory frameworks that companies navigate.
According to a study AWS has commissioned from Strand Partners, to drive AI adoption across the EU's economy, European policymakers must foster a harmonized regulatory environment that reduces compliance costs, which are currently estimated at 40% of IT expenditures for companies. Furthermore, 59% of startups report delaying AI plans due to regulatory concerns and 44% of European businesses cite regulatory uncertainty as their primary barrier to AI adoption. While growth rates are estimated at 30% (as also found in the latest Digital Decade report), there remains a challenge in maintaining and accelerating that growth to meet the 75% target by 2030. We therefore recommend that the Commission prioritizes measures to stimulate the uptake of cloud and AI, focusses on making the current regulatory framework a success and refrains from introducing new regulatory requirements without carefully assessing whether existing concerns can be mitigated through the enforcement of existing rules.

Conclusion

The proposed EU Cloud and AI Development Act can represent an important milestone in Europe's digital transformation journey. As the EU seeks to address its infrastructure capacity gaps and strengthen its digital sovereignty, it must carefully balance ambitious goals with practical implementation. The success of this initiative will largely depend on its ability to streamline administrative processes, harmonize existing regulations, and create an environment conducive to sustainable growth and innovation.

The path forward requires a pragmatic approach that prioritizes the removal of current bottlenecks in data center development while leveraging existing regulatory frameworks. Rather than introducing new layers of complexity, the Act should focus on simplifying permitting processes, addressing grid connection

challenges, and aligning with established sustainability standards. The framework should recognize that security and sovereignty assurances can be achieved through robust technical and organizational controls, without resorting to restrictive ownership-based criteria that might limit innovation and customer choice. Particularly important is the need to avoid regulatory duplication and instead ensure effective implementation of existing frameworks such as the Data Act, DORA, and NIS2. This approach aligns with the Commission's broader regulatory simplification agenda while maintaining high standards for security and operational resilience. For public sector adoption, the focus should be on developing inclusive procurement guidelines that encourage competition and innovation while maintaining appropriate safeguards for sensitive use cases.

Looking ahead, the success of this initiative will be measured not just by the growth in infrastructure capacity, but by its ability to enable European organizations to compete effectively in the global digital economy while maintaining control over their critical data and operations. By focusing on practical measures that accelerate deployment while preserving market dynamics, the EU can create a framework that truly serves its digital transformation goals and strengthens its position in the global technology landscape.