EUROPEAN
COMMISSION

Brussels, 3.6.2026
SWD(2026) 502 final

PART 1/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

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

Table of contents

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT 4
   1.1. Political context 4
   1.2. Legal context 5
2. PROBLEM DEFINITION 6
   2.1. Problem context 6
   2.2. What are the problems? 9
   2.3. What are the problem drivers? 15
   2.4. How likely is the problem to persist? 25
3. WHY SHOULD THE EU ACT? 26
   3.1. Legal basis 26
   3.2. Subsidiarity: Necessity of EU action 27
   3.3. Subsidiarity: Added value of EU action 27
4. OBJECTIVES: WHAT IS TO BE ACHIEVED? 28
   4.1. General objectives 28
   4.2. Specific objectives 28
5. WHAT ARE THE AVAILABLE POLICY OPTIONS? 29
   5.1. What is the baseline from which options are assessed? 29
   5.2. Description of the policy options 31
   5.3. Options discarded at an early stage 56
   5.4. Possible combination of options 56
6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS? 57
   6.1. Economic impact 57
   6.2. Social impact 73
   6.3. Environmental impact 74
7. HOW DO THE OPTIONS COMPARE? 78
   7.1. Effectiveness 78
   7.2. Efficiency 85
   7.3. Coherence 86
   7.4. Subsidiarity and proportionality 89
   7.5. Sensitivity analysis 89
   7.6. Comparison per criteria 90
8. PREFERRED OPTION 93
   8.1. Outcome of comparison of policy options 93
   8.2. Application of the “One In One Out” (OIOO) Approach 95
9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? 97

ANNEX 0 - ENDNOTES 100

Glossary

Term or acronym	Meaning or definition
AI	Artificial Intelligence
AZ	Availability Zone
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CfE	Call for Evidence
Colocation data centre	A data centre in which one or more customers install and manage their own network or networks, servers and storage equipment and service
Colocation data centre operator	An organisation who manages and leases/sells space, security, network access, power and cooling capacity from a colocation data centre to one or more customers who install and manage their own network or networks, servers and storage equipment and services
CSP	Cloud service provider
Data Centre (DC)	A data centre (DC) is defined as a structure or a group of structures used to house, connect and operate computer systems/ servers and associated equipment for data storage, processing and/or distribution, as well as related activities.
DSO	Distribution System Operators operate and manage local and regional distribution networks, delivering electricity to end users from the transmission system, such as Data Centres up to a given size. See also TSO.
EC	European Commission
Enterprise data centre operator	Enterprise data centre operator is a physical or legal person who manages the entire enterprise data centre, including the building and the use of the information technology services delivered
EED	Energy Efficiency Directive
EU	European Union
FLAPD	Refers to the data centre markets located in Frankfurt, London, Amsterdam, Paris and Dublin.

FTE	Full Time Employee
Hyperscaler	Hyperscalers are very large cloud and AI computing service providers. They are characterized by their ability to provide cloud computing at very large scale. Hyperscalers include Amazon (Amazon Web Services), Microsoft (Azure), and Google (Google Cloud Platform).
IA	Impact Assessment
ICT	Information and Communication Technology
IPCEI	Important Project of Common European Interest
MS	Member State(s)
OSS	Open Source Software is software that is released under a license that allows users to view, modify, and distribute the source code.
PUE	Power Usage Effectiveness, or PUE, is a metric used to measure the energy efficiency of data centres. It is defined as the ratio of total facility energy to the energy used by IT equipment. A PUE of 1.2 implies that for each unit of energy spent in powering IT equipment, 0.2 units are spent for non-IT equipment such as cooling. A lower PUE indicates better energy efficiency, as it means less energy is being used for non-IT purposes.
Simpl	Smart middleware platform for data spaces
SME(s)	Small- and Medium-sized Enterprise(s)
TFEU	Treaty on the Functioning of the European Union
TS	Technical Specification
TSO	Transmission System Operators, or TSOs, manage the high-voltage transmission networks that transport electricity over long distances, ensuring stability and reliability across regions. Above a given size, Data Centres connect to the grid directly through TSOs. See also DSO.

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Today, cloud computing and AI are more than enablers of innovation. They have become the driving forces reshaping industry, public service, and daily life in the EU. The cloud provides the backbone necessary for all to access and deploy digital solutions efficiently, while AI unlocks unprecedented opportunities for automation, data-driven decision-making, and personalised services. A strategic approach to their uptake is thus essential for a competitive, secure, sovereign and future-ready EU. Annex 8 explains the technical terms used in this assessment such as the notion of cloud and AI computing services, which, in the context of this assessment, means offering computing resources for the running (inference) of AI systems.

1.1. Political context

The Draghi report on the future of European competitiveness[i] recognised the importance of sufficient access to cloud services and of increasing computational capacity in the EU, particularly for the EU's ability to develop and adopt AI[ii]. The Competitiveness Compass calls for the EU to provide sufficient cloud and data infrastructure required for AI leadership, as enablers of competitiveness[iii]. The Economic Security risk assessment on AI technologies identified dependencies on a limited number of foreign cloud providers and frontier AI providers as significant vulnerabilities in the European AI ecosystem[iv]. The Cloud and AI Development Act (CADA) is a headline digital policy initiative listed in the Mission letter to EVP Virkkunen, alongside a single EU-wide cloud policy for public administrations and public procurement[v]. The Competitiveness Compass calls for action in Europe to provide sufficient cloud and data infrastructure required for AI leadership, as enablers of competitiveness[vi]. Furthermore, the AI Continent Action Plan[vii] announces the goal of tripling the EU's data centre (DC) capacity within the next five to seven years and emphasises that sovereignty and operational autonomy need a greater reliance on highly secured EU-based cloud capacity. The Digital Decade Policy Programme (DDPP) sets the target of 75% of EU businesses adopting cloud services and of 10 000 edge nodes being rolled out by 2030[viii].

The **European Parliament**'s own-initiative report (tabled for plenary since June 2025) on European technological sovereignty and digital infrastructure voices concerns about the EU's excessive dependence on non-European actors in critical areas like cloud infrastructure. It calls on the Commission to introduce the CADA to strengthen European data infrastructure, promote European cloud service providers (CSP), build a European single market for cloud and AI, and propose a definition for sovereign cloud and its scope of application[ix]. In its conclusions of December 2025 on European Competitiveness in the Digital Decade, the **Council** calls for CADA to include *common criteria for sovereign cloud services, allowing for addressing market transparency and risks associated with dependencies, including extraterritorial effects of legislation adopted by third countries for highly critical use cases*[x].

Several non-EU countries have adopted policy initiatives to develop AI computing capacity, including DCs. In the **US**, building on a long tradition of supporting their cloud sector with policies[xi] and large public contracts[xii], the July 2025 AI Action Plan[xiii] massively boosts US DC capacity and cloud services. An Executive Order on accelerating federal permitting of DC infrastructure[xiv] establishes nation-wide fast-track procedures, lowers environmental protections, and makes federal land available for DC build-out. The Executive Order on promoting the export of the American AI Technology Stack establishes federal support for full-stack AI export packages bundling AI-optimised computer hardware, DC storage, cloud services, and networking, which will be exclusively sold in US-providers-only packages[xv]. **China** launched the infrastructure project "Eastern Data, Western Computing" in 2022, coordinating DC construction by concentrating facilities in the West of the country. This led to a surge in government procurement of DCs[xvi]. In July 2025, the **UK** proposed AI Growth Zones to better equip the UK

for running training and inference and support UK companies in developing sovereign, sustainable and secure compute technologies and services[xvii]. The **UAE** pursues investments in renewable energy, power transmission, and hyperscale-ready infrastructure to expand its DC capacity[xviii].

1.2. Legal context

The EU lacks a framework to foster the strategic investment in computing capacity beyond AI Factories and Gigafactories[1]. The DDPP[xix] only sets a deployment target for edge nodes, but not for DCs. The legislative framework for DCs focuses on enhancing their sustainability through transparency measures without explicitly incentivising deployment. The Energy Efficiency Directive (EED)[xx] establishes an annual sustainability reporting and lays the basis for a rating scheme. The Taxonomy for Sustainable Finance enhances transparency on DC sustainability for financial market participants[xxi]. DCs must comply with minimum performance and information rules of the Ecodesign Regulation[xxii]. While DC projects are not subject to mandatory environmental impact assessments based on EU rules, such assessments are often required by Member States[2]. The upcoming Industrial Accelerator Act will create clusters for accelerating industrial activity for the manufacturing sector, from which DCs will not benefit. Other EU initiatives target key input factors for DC deployment: the upcoming Digital Networks Act[xxiii] will improve connectivity; the Grids Package[xxiv] will ensure that electricity grids can serve growing demands, with focus on improving permitting, planning but also providing tools to accelerate grid connections procedures via a dedicated guidance on grid connections; the Savings and Investments Union[xxv] will improve access to capital in the EU. While these frameworks can benefit DC deployment, they are not tailored to the sector's specific needs. The upcoming Regulation on accelerating and streamlining environmental assessments establishes a toolbox with provisions for faster environmental assessments, applicable to strategic sectors when sectoral legislations refer to it, something that CADA will leverage for DC projects.

Similarly, the EU lacks a framework for incentivising the uptake of European cloud and AI computing services and for ensuring security of supply. The DDPP sets high-level adoption targets[3], and the Apply AI strategy[xxvi] supports AI adoption in strategic sectors, but without concrete measures geared at European services. Other existing frameworks address market practices: the Data Act[xxvii] regulates cloud switching and interoperability. The Digital Markets Act[xxviii] considers cloud services as core platform services where providers can be designated as gatekeepers and subject to specific obligations[4]. The Digital Networks Act will address the scenario where a CSP operates a connectivity network. The AI Act[xxix] sets out risk-based rules for providers and deployers of AI systems and general-purpose AI models, fostering trustworthy AI but without addressing computing. Other frameworks address cybersecurity: the Cybersecurity Act (CSA)[xxx], currently under review, enables the adoption of an EU-wide cybersecurity certification scheme for cloud services[5] and addresses supply chains by tackling high-risk vendors but without addressing public procurement. The Digital Operational Resilience Act[xxxi] targeting financial entities, and the NIS2 Directive[xxxii] defining sectors of high criticality, require entities like CSPs to implement risk management and other security measures. The use of cloud and AI computing services in the public sector is horizontally governed by the Public Procurement framework, currently under revision, which enshrines transparency, equal treatment, open

[1] These initiatives focus on High Performance Computing (HPC) and do not address the need for more decentralised computing capacity.
[2] According to the Environmental Impact Assessment (EIA) Directive, changes to which may come from the Environmental Omnibus: Directive - 2014/52 - EN - EIA - EUR-Lex.
[3] 75% business adoption of cloud, AI, or big data by 2030.
[4] So far, no provider has been designated as a gatekeeper for the provision of cloud services, but on 18 November 2025, the Commission opened three market investigations on cloud computing services under the DMA.
[5] This requires an Implementing Regulation. ENISA has been working on developing the European cybersecurity certification scheme for cloud services (EUCS) since 2019, which has not been adopted yet. Two technical specifications by CEN-CENELEC have resulted from this work on the security requirements and the accreditation of the conformity assessment bodies and the conformity assessment methodology.

competition and sound procedures as well as respect for EU's international commitments[xxxiii]. However, these initiatives fall short of addressing sovereignty considerations in this sector.

2. PROBLEM DEFINITION

The analysis conducted identified two key problems that warrant policy attention. This chapter presents these problems in detail, exploring their underlying root causes structured around four main problem drivers. It further assesses the associated risks and potential consequences should these issues remain unaddressed. To better define and characterise the identified problems, it is useful to first examine the competitive dynamics in the cloud computing market and the functioning of cloud service demand and supply, as a critical contextual element.

2.1. Problem context

Cloud computing emerged in the early 2000s in the United States, with Amazon Web Services (AWS) being established in 2002 and commercial cloud offers from AWS, Google and others becoming popular from 2008 onwards. The early 2010s set the stage for the massive adoption of cloud services[xxxiv], which accelerated further in subsequent years. The global cloud and data infrastructure market grew by around 35% per year since 2016[xxxv], with expected growth rates above 20% for subsequent years. In the EU, this high-growth environment led the share of enterprises buying cloud services to increase from 18% in 2014 to 53% in 2025, with adoption almost tripling in a decade; for large firms, the figure exceeds 80%[xxxvi]. This rapid growth in market demand can be linked to three major trends:

- The digitalisation of the economy and a structural shift from on-premises IT models: businesses across sectors have migrated from traditional on-premises infrastructure to cloud solutions, considered to offer lower upfront costs, more flexibility and a richer ecosystem of services in a single interface. Part of this cloudification has also been supply-driven, as providers pushed from installed licences to cloud subscription models[6]. Major CSPs, massively supported by system integrators, expanded their service portfolios, pricing models and migration programmes in ways that created and deepened the demand for cloud services. This initial trend from on-premises to infrastructure-as-a-service (IaaS) has seen a second wave towards more advanced platforms deployed as platform-as-a-service (PaaS) and software-as-a-service (SaaS). The growing weight of PaaS and the shift towards AI (mostly deployed as SaaS) has been a key market dynamic in the last years and remains so to date.
- The emergence of new cloud native digital services: demand has increased with the rise of cloud-native platforms such as social media, video and music streaming, and a broad range of SaaS applications such as Customer Relations Management tools.
- Artificial Intelligence and data-driven business models: the diffusion of AI, advanced analytics and data-intensive applications have increased demand for compute power, often requiring processing capacity close to end-users to meet low-latency requirements, thus reinforcing the shift towards cloud and edge solutions.

From 2017 to 2021, the European cloud market expanded rapidly, notably during Covid-19, which increased the use of digital services and boosted demand for cloud computing across the EU. However, most of the incremental demand was captured by US hyperscalers, whose share rose from around half to two-thirds of the market, while European providers' collective share nearly halved[xxxvii]. During this period, European CSPs were predominantly national or regional players serving domestic markets. They reacted to foreign competition by either specialising in use cases

[6] For example, Office 365 monthly active users grew from around 60 m in 2015 to 200 m in 2019, while traditional Office product revenues fell by around 21%. See: Office 365 Number of Users Reaches 345 Million Paid Seats and FY23 Q4 - Productivity and Business Processes Performance - Investor Relations - Microsoft

with stronger data sovereignty and privacy demands[xxxviii] or by developing partnerships with the hyperscalers[7], rather than matching the broad footprint of US providers. This was the case too of European Telco providers who ventured into cloud services, but mostly partnering with US CSPs, becoming de facto resellers. The 2021 European industrial technology roadmap for the next generation cloud-edge offering, prepared by key European players, argued that the European digital market was "*fragmented into local realms, individually lacking the critical mass for players to scale and compete*" with the US and China[xxxix]. Despite strong revenue growth, the market share of European providers declined. By contrast, large US providers have been able to benefit given their early, large-scale deployment of cloud offerings, which put them in a position to capture this market growth. This was made possible by three elements.

Firstly, US CSPs were able to build on an early growth driven by US government adoption. In 2013, the Central Intelligence Agency awarded a USD 600 m contract to AWS[xl], followed by the award of a fifteen-year multi-billion-dollar contract for the development of the "Commercial Cloud Enterprise" to AWS, Google, IBM, Microsoft and Oracle. The Department of Defence awarded additional sizeable contracts to these providers for developing secure cloud services or enabling the migration to the cloud of agencies like DARPA[8]. These early and large-scale public contracts ensured fixed revenues and allowed these providers to grow their portfolio, often with particularly secure services resulting from the stringent requirements of the US administration. These providers carried their first-mover advantage to Europe demand for cloud services was just emerging[xli], driving early European cloud users to turn to US providers[9]. As well, in the shift from on-premises to cloud solutions, hyperscalers extensively used partner networks. By offering dedicated training and skill certifications, they engaged in partnerships with consulting firms and resellers, through which they could rapidly expand in local markets[xlii].

Secondly, the absence of a thriving tech industry in the EU prompted US CSPs to leverage their domestic advantage by partnering with large global technology companies when expanding into the European market. Indeed, figures show that cloud adoption in the EU is driven by companies working in the ICT sector[xliii], which are often not European and tend to buy the same cloud services as they buy domestically, i.e. US CSPs. Some examples: Netflix, which serves more than 50% of the European video-on-demand market, relies exclusively on AWS for its core cloud infrastructure[xliv]; the Amazon (retail) Marketplace serves as an anchor customer for AWS, its own cloud services offering.

With respect to market dynamics, competition in cloud services, like other capital-intensive network industries, is characterised by distinct supply and demand side elements.

On the supply side, cloud markets are defined by considerable sunk costs associated with data centre deployment, with long investment times and substantial economies of scale and scope. These characteristics tend to benefit large providers which can fund expensive compute capacity and distribute costs across a wide customer base and a diverse service portfolio. When looking at infrastructure, high fixed costs constitute a major barrier to entry. The cloud and AI infrastructure market is capital-intensive: building and equipping data centres requires large upfront investment, and providers are able to secure financing if they expect sufficient demand and market share gains. Differences in deployment procedures among Member States create transaction costs within the single market, affecting the profitability of new projects. These costs are more easily absorbed by

[7] For example, German provider plusserver working with AWS, Azure and Google Cloud in 2019 by offering hybrid solutions interconnected with hyperscalers. See: https://www.juniper.net/content/dam/www/assets/case-studies/us/en/plusserver.pdf

[8] An excerpt of awarded contracts from different US Departments and agencies to US hyperscale cloud providers: C2E - $600 m (CIA, 2013-present), Wild & Stormy – USD 10 bn (NSA, 2021 – 2023), JWCC – USD 9 bn (DoD, 2022 – 2028). See also : DARPA plans shift from AWS and on-prem to fully cloud by 2022; General Dynamics again wins DOD's cloud email & collaboration contract; Big Tech and the US Digital-Military-Industrial Complex - Intereconomics.

[9] In the Netherlands, for example, the strong reliance of the public sector on hyperscalers is laid down by the Netherlands Court of Audit, which analyses selected critical cloud contracts awarded by the Dutch central government.

larger providers but remain prohibitive for smaller firms. Access to funding is also slower and more complex for small enterprises. By contrast, AWS, Microsoft and Google were able to collectively invest around EUR 12 bn in European infrastructure in 2020 alone, marking a 20% increase compared to the previous year[xlv]. This investment capacity was underpinned by vertically integrated businesses and diversified revenue streams. The French Autorité de la Concurrence, in its 2023 opinion on cloud services, emphasised that hyperscalers benefit from "conglomerate" structures, i.e. their presence in multiple digital markets allows them to develop credit systems and discounts using their market power to accelerate cloud growth. Similarly, a more recent work by the OECD on competition in the cloud market notes that hyperscalers are best equipped to mitigate the risks of aggressive cloud expansion by "portfolio diversification or cross-subsidising losses"[10]. On the innovation side, the asymmetry with European players is also evident. The EU Industrial R&D Investment Scoreboard showed that by 2018-2020 Amazon, Alphabet and Microsoft were among the top global corporate R&D investors, each spending in the order of billions of dollars per year. In the same period, Europe's largest R&D spenders were concentrated in the automotive and pharmaceutical sector, while European cloud providers like OVHcloud were small companies with revenues in the hundreds of millions and modest R&D budgets[xlvi]. This disparity in innovation spending, combined with hyperscalers large capital expenditures, projected to reach USD 335 bn in 2025[xlvii], has given them an important advantage over smaller providers to offer broader service portfolios and integrated ecosystems.

On the demand side, customer choices are shaped by two key factors: the value placed on flexibility and the breadth of services available through single platforms operating seamlessly. On these two key factors, hyperscalers have been better placed than European providers from the start. Although European cloud offerings encompass a diverse range of services, customers need to collaborate with multiple providers to match the quality and breadth of services offered by leading global cloud providers. End-users desire simplicity and have grown accustomed to one-stop shops delivering everything from Infrastructure-as-a-Service (IaaS) to Software-as-a-Service (SaaS) on a global scale, a level of integrated service that hyperscalers readily supply. In contrast, European providers typically have more limited catalogues, often focused on specific infrastructure or industry niches, making it challenging to secure substantial, multi-country enterprise deals. In several European industries, value chains are organised around networks of smaller providers that combine their specialised products across the single market, supported by common standards and technical specifications. This was achieved in the telecom sector after the introduction of the GSM standard. However, a similar market structure has not materialised in the cloud sector. As mentioned above, instead of pooling resources and federating, European providers decided to (i) build partnerships with US hyperscalers, (ii) focus on a specific region, or (iii) specialise in a single layer of the cloud stack, e.g. IaaS or Saas offerings, rather than offering a comprehensive portfolio. By contrast, US hyperscalers deliver an integrated, end-to-end service, operating as "IT supermarkets"[xlviii]. The French competition authority clearly noted that hyperscalers' large ecosystem of offers implies that, for several workloads, competition takes place "for the market" rather than "on the market" as customers tend to choose a single supplier able to cover their entire needs.

The repercussions of these competition dynamics result in a rigidity when it comes to switching providers and considering alternative offers. Leading providers impose complex pricing structures, egress fees and restrictive licensing terms. When switching providers, customers face high costs stemming from egress charges, the use of proprietary data formats or APIs and long-term contracts[xlix], i.e. different forms of vendor lock-in[l]. Even if a better or cheaper provider exists, customers may therefore not switch, weakening competitive pressures and resulting in alternative

[10] OECD, "Competition in the provision of cloud computing services"

providers struggling to attract customers due to factors outside of their control[11]. The Dutch competition authority's cloud market study concludes that users encounter technical hurdles to portability and incur significant financial costs for data transfer, which collectively make switching providers challenging and effectively lock users into the chosen cloud provider for lengthy periods, contributing to market consolidation[li]. Moreover, once a provider becomes the 'default' or 'safe choice', the customer starts creating the tooling and culture around this provider, resulting in inertia as an effective blocker of new incumbents. In this context, EU providers struggle to attract customers away from well-established US providers. The challenges described above, along with difficulties in partnering with system integrators, consultancies and intermediaries to promote European solutions, have collectively contributed to the gradual erosion of market share for EU CSPs.

Last but not least, there are signals of new opportunities for European providers to gain market shares. AI adoption, the third demand driver identified above, is bringing change to the market landscape, and competitive positions could change. While US providers are already well established mostly thanks to their integrated offers, European providers might still find opportunities to capture growth, especially in relation to more specialised, sector-specific offers, where their proximity to customers and ability to provide safeguards in terms of data localisation and integrity are important. The Apply AI strategy adopted by the Commission is a signal in that direction. AI has the potential to alter industry business models, with cloud and AI services extending beyond basic IT commodity functions to become integral parts of a company's competitive edge. Furthermore, the issue of sovereignty, exacerbated by geopolitical considerations, has gained prominence and could be an opportunity for European cloud and AI providers. According to Gartner[lii] the sovereign cloud IaaS market is forecast to grow at a yearly rate of 38% in the next five years, with developments in terms of moving away from global cloud providers and new business migrating to a sovereign cloud environment. The positioning of European cloud and AI providers as sovereign is, however, today hindered by a lack of clarity and lack of harmonisation in the market in terms of how sovereign services are defined.

2.2. What are the problems?

2.2.1. Problem 1 - Limited and geographically concentrated availability of computing capacity in the EU

AI is driving an unprecedented demand for computing capacity, not only for the High-Performance Computing (HPC) capacity required to train models, but also for the capacity to enable inference, fine-tuning and service integration[liii]. The European AI market is projected to exceed EUR 300 bn by 2030[liv], growing at more than 26% between 2025 and 2030[12]. Beyond AI, adoption of cloud computing and other digital services continues to accelerate, adding further pressure on the available computing capacity[13]. In 2025, uptake of new DC capacity in Europe[14] is expected to reach a new high of 854 MW[15], exceeding new supply for the third consecutive year[lv]. Vacancy rates in major EU DC hubs have declined to historical lows, and the share of co-location

[11] While these contextual factors are referred to in the problem drivers described below, they are not themselves considered as drivers for this analysis as they are addressed through a dedicated intervention under the Data Act (see section 7.3 and annex 7) and through competition cases. See for example the European Commission's investigation into Microsoft Teams: Statement of Objections to Microsoft.

[12] Enterprise adoption of AI technologies remains limited at 13.5% according to the latest data from the Digital Decade Policy Programme, partly due to infrastructure constraints and cost barriers. The Digital Decade 2025 report highlights the need for the data centre industry to expand and adapt to support the rapid growth of AI technologies.

[13] In 2025, per Eurostat, EU business cloud uptake stood at 52.7% - far from the 2030 target of 75%, but that also includes the adoption of cloud, AI or data analytics. As more European businesses adopt cloud and AI computing services, demand for DCs is thus expected to rise further.

[14] When looking at the DC market, Europe typically includes the UK.

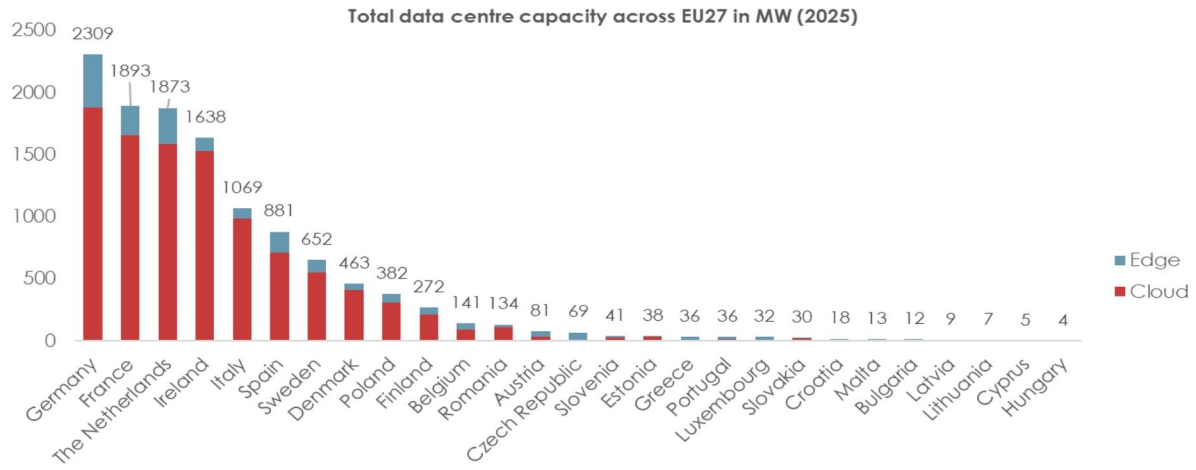
[15] DC capacity is typically expressed in megawatts (MW) or gigawatts (GW) because power availability plays a key role for both the operation of the servers and the cooling systems.

capacity that is pre-leased[16] before becoming operational continues to rise. These are clear signs of high demand[lvi].

Across the EU27, **the expansion of data centre capacity is not keeping pace with this rapidly growing demand.** Despite increased investment[lvii] and installed capacity expected to reach 12.4 GW in 2025[17], available supply remains insufficient, resulting in an estimated gap of almost 3 GW relative to current demand.

Moreover, **the existing capacity is concentrated in a limited number of established hubs**, mostly in Northern and Western Member States: in 2025, Germany (Frankfurt), France (Paris), the Netherlands (Amsterdam) and Ireland (Dublin) account for 65% of the EU27 DC market[18] (Figure 1[19]). These locations have historically provided more favourable factors for DC deployment, e.g. strategic geographic location, proximity to end users, and connectivity to other world regions. Ireland, for example, is geographically positioned as a gateway between Europe and the US, with extensive undersea fibre-optic cable networks. This makes it an ideal location for low-latency transatlantic data transfers for US CSPs serving European markets from overseas. Ireland's low corporate tax rate and supportive government policies have attracted significant foreign direct investment, particularly from US tech companies. These companies, including the cloud hyperscalers, have established major operations in Ireland, contributing to the rapid expansion of nearby data centre infrastructure[20].

Figure 1. Data centre capacity across EU 27 MS in 2025



Source: Technopolis et al. (2025)[lviii]

Expressed per 100 000 inhabitants, overall capacity amounts to 2.75 MW per 100 000 people and is concentrated in a few Member States, with Ireland, the Netherlands, Denmark, Sweden, Finland and Luxembourg standing out (

Figure 2).

[16] Pre-leased capacity in DC means that customers commit to renting space and power before the facility becomes operational. Market information points to a growing share of data centre spaces already reserved before delivery, reflecting very high demand and tight supply.

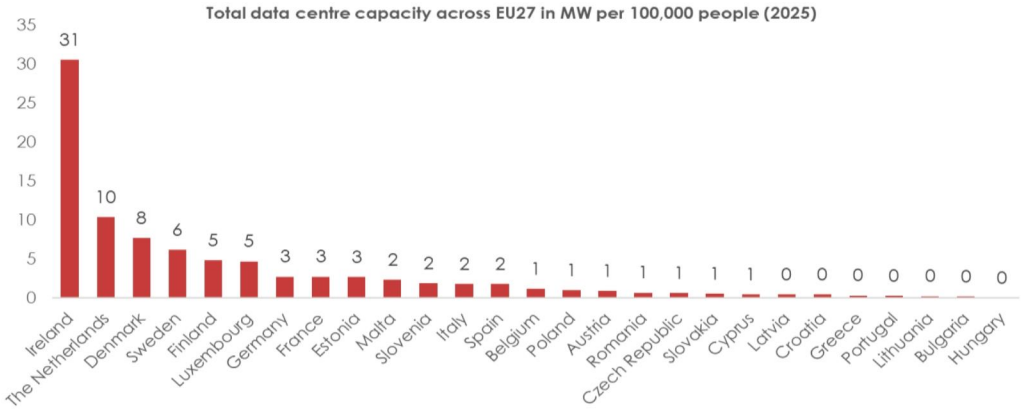
[17] Technopolis Group, Wavestone, Timelex, STL Partners, OpenForum Europe and KAPA Research (2025), "Study: Cloud and AI". The methodology is based on all known commercial data centre sites listed in the *Data Center Map*, additional sites identified through the survey and any publicly known hyperscaler sites. The figures do not include private enterprise sites, under which most dedicated HPC facilities fall.

[18] Technopolis Group et al. (2025), "Study: Cloud and AI".

[19] Core EU DC hubs include Frankfurt, Amsterdam, Paris and Dublin. This concentration is explained by operators leveraging metro areas and exploiting the best locations in terms of connectivity (Dublin, Paris, Frankfurt, Amsterdam), proximity to economic hubs (Paris, Frankfurt, Amsterdam) or low corporate tax (Dublin).

[20] In a second phase, hyperscalers made substantial investments in locations with strong sectoral demand, such as Frankfurt for banking services and Belgium for the pharmaceutical industry.

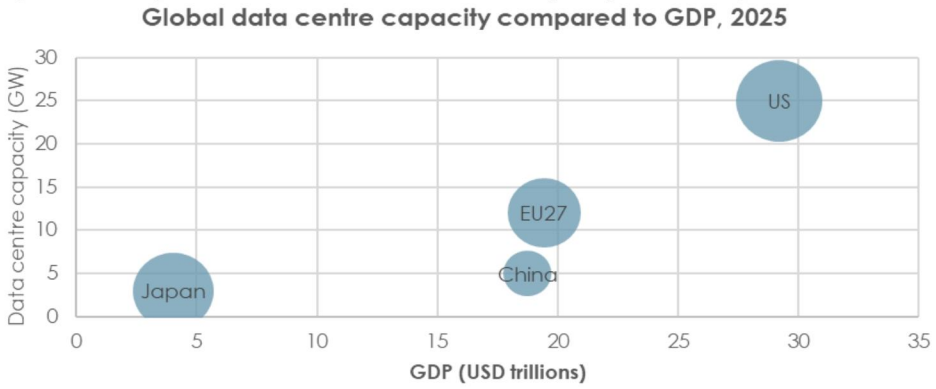
Figure 2. Data centre capacity per 100 000 people across EU 27 MS in 2025



Source: Technopolis et al. (2025)[lix]

In addition, the EU lags behind other regions in both scale and ownership of digital infrastructure (see Figure 3). In 2022, Europe had approximately 1 MW of installed data centre capacity per 100 000 people, while the US had 12 MW[lx]. The situation persists today: despite similar GDPs, in 2025 the EU accounts for only 20% of global installed data centre capacity compared to the US (42%)[lxi].

Figure 3. Comparison of GDP and data centre capacity for leading markets in 2025



Source: Technopolis et al. (2025)[lxii]

The existing capacity gap and strong geographical concentration point to structural inefficiencies in the allocation of resources in the market for data centre capacity, with effects already visible today:

The limited supply has led to rising prices for existing capacity, negatively affecting businesses which rely on such capacity. Since 2022, average asking prices in the European colocation markets have increased by 51% for 100 kW leases [lxiii]. New co-location capacity is often leased to large service providers: Amazon Web Services (AWS), Microsoft, Google[21]. By 2028, they are expected to drive 65% of the demand for DCs in Europe, an increase of 12% during the same timeframe[lxiv]. This reinforces the competition dynamics discussed above: when most of the new capacity is effectively reserved by a handful of players, they can shape where and how new infrastructure is built, secure access to suitable sites and further capitalise on economies of scale. Already today, vacancy rates in Europe's top DC markets are at a record low of 7.4%[lxv]. Due to a lack of available space, co-location providers are expected to raise prices in 2025 by 10% in leading DC markets[lxvi]. The negative effects on businesses' ability to access capacity are

[21] Co-location data centre operators often lease their facilities to hyperscalers to obtain a quicker return on investment.

particularly pronounced in regions with a high concentration of DCs, where businesses are faced with higher prices.

As noted above, geographic concentration puts a strain on affected regions: in Ireland, DCs accounted for 22% of electricity demand in 2025, up 5% from 2015. The resulting grid stress has led local TSOs to enact a de facto moratorium for new DC applications in Dublin due to fears of overloading the grid and compromising energy security[lxvii]. Municipalities in Noord-Holland have also enacted several moratoria on building new DCs, the latest one in 2023 in Amsterdam[lxviii]. In the case of Dublin, the moratorium has reportedly stalled EUR 8-10 bn in planned DC investments. The effects of grid stress also impact other user groups[22]. In Luxembourg, the plans for a large DC by Google have been subject to a review of its energy grid planning that includes a new connection to Germany[lxix] because local electricity generation was not sufficient. This situation, with the saturation of existing infrastructure, has further slowed deployment, raised energy system pressures and diverted investment, rather than leading to an efficient redistribution of capacity across the Union.

While cloud and AI computing services can be technically delivered cross-border, regions with a low DC presence are also disadvantaged by this geographic imbalance, as exemplified by the higher prices in regions with low DC presence[lxx]. Moreover, the lack of nearby computing capacity drives up latency, limiting the availability and quality of low-latency services, thus placing local end-users at a competitive disadvantage compared with regions that have better access to DC capacity[23] (see also section 2.3). It also points to under exploited investment opportunities if comprehensive business cases can be built around these cases. Over time, this can slow digital transformation in the affected Member States and weaken overall competitiveness within the Digital Single Market. Stakeholders have also warned that this limited availability of computing capacity in the EU acts as a barrier for the development and uptake of cloud and AI computing services: for instance, Mistral AI has warned that a lack of DC capacity could become a roadblock for developing and applying AI models in Europe[lxxi]. Current market dynamics risk reinforcing existing concentrations, increasing regional disparities and limited access to computing resources for business and public authorities outside main hubs.

2.2.2. Problem 2 - Dependence on cloud and AI computing services supplied by non-European[24] providers

The European cloud services market is growing significantly. It was worth around EUR 70 bn in 2022 and is estimated to reach over EUR 200 bn by 2028[lxxii]. In 2024, the European Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) market was dominated by three US companies, the so-called hyperscalers (Table 1). Worldwide, AWS held a market share of 32% in Q2 2024, Microsoft 23% and Google Cloud 12%. No other provider held more than 4%[lxxiii].

In Europe, those three providers account for around 70% of the market, while the largest European providers (SAP and Deutsche Telekom) each serve 2%[lxxiv]. The European cloud market has grown, but the market share of European providers has decreased from 29% in 2017 to 15% in 2022 and has since remained stable[lxxv]. A recent study for the European Parliament reaches the same conclusion, noting that US firms dominate all major software layers, including cloud, and that European providers account only for a small share of the infrastructure market[lxxvi]. Despite

[22] In Ireland, for example, interest representatives point to increasing delays for electricity connection of housing projects: Govt warned of rising household bills as data centres strain grid.

[23] Taking the example of Microsoft's Azure regions, round-trip latency (the time it takes for a data pack to travel from one point in the network to another and back again) from Poland (Central Europe) to Frankfurt (Western Europe) is ca. 10–15ms, and latency from Poland to Amsterdam or London is ca. 15–20ms. By contrast, latency within Western Europe (e.g. Frankfurt to Amsterdam) is typically <5ms. A fintech business in Warsaw thus faces significantly higher latency than a competitor in Western Europe.

[24] Whereas section 2.1.1. deals with the presence of computing *capacity* in the EU, including capacity provided by non-EU companies; this section deals with *services* provided by companies headquartered in the EU.

European providers playing an important role in some Software as a Service market segments, non-EU providers dominate in important fields, such as office automation and productivity software[25].

Table 1. Market leaders for cloud services (IaaS, PaaS and hosted private cloud revenues), Q2 2024

	World	US	China[26]	Rest of APAC	**Europe**	Rest of World
#1	Amazon	Amazon	Alibaba	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Tencent	Microsoft	Microsoft	Microsoft
#3	Google	Google	China Telecom	Google	Google	Google
#4	Alibaba	Oracle	Huawei	NTT	Oracle	Salesforce
#5	Oracle	Salesforce	China Unicom	Alibaba	Salesforce	Oracle
#6	Salesforce	IBM	China Mobile	Fujitsu	IBM	IBM

Source: Synergy Research Group

Hyperscalers thrive in the European cloud market thanks to their global scale, significant financial resources, and overall ecosystem gravity, composed of integrated digital ecosystems[lxxvii], partnership programmes and marketplaces, among others.

On the supply side, this problem impacts European providers of cloud and AI computing services in terms of foregone commercial opportunities. Astères approximates their magnitude by estimating that EU companies' annual purchases of cloud software add EUR 264 bn to the US economy[lxxviii]. On the demand side, this problem impacts private and public sector users of cloud and AI computing services. Some reports suggest that, by relying so strongly on a small number of providers, users pay more for their cloud and AI computing services than by relying on alternatives[27]. In its most basic form, this dependence can lead to significant economic costs. Without alternative, users are defenceless in light of price increases. This is illustrated by Broadcom's acquisition of VMWare (a provider of leading virtualisation technology, for which little European alternatives exist), which resulted in unilateral licensing changes and price increases of 800% to 1500% according to users[28]. More generally, there is evidence suggesting that the dependence on non-European providers may cause European users to over-pay, with some reports suggesting that European providers offer digital resources at lower prices[29] and with lower egress charges.

European AI computing service providers lag their global competitors[lxxix,] also due to their competitive disadvantage in accessing computing service providers[lxxx].

Dependence also introduces significant tail risks: where users rely on a small number of providers, cloud outages can have far-reaching consequences, including business interruptions, and substantial financial or data losses[lxxxi]. Strong reliance on a small set of providers also means that a single failure can simultaneously affect several critical services, as seen in the recent Crowdstrike incident or AWS outages[lxxxii]. It also limits the EU's operational autonomy and system resilience as these providers may be exposed to third-country policies restricting service access, for example in the context of sanctions or economic coercion. This risk recently materialised in the suspension of service provision to the Chief prosecutor of the International Criminal Court, on whom the US had previously imposed sanctions[lxxxiii]. This case illustrates the challenges which exposure to third-country policies can cause to operational autonomy and system resilience in the EU. Another illustrative example is the planned takeover of the Dutch cloud provider Solvinity by the US IT

[25] For example, in 2023, SAP held 49.6% of the specialised market for Travel and Expense Management Software.
[26] In China, foreign invested companies are not allowed to provide so-called Internet Data Centre Services according to the Promulgating the Classification Catalogue of Telecommunications Services and must rely on local Chinese partners in the form of a technology cooperation.
[q] For example, Leitmotiv Digital finds that European providers offer digital resources at prices that are five to ten times lower than the current incumbents: Leitmotiv - Toward our Digital Future.
[28] https://www.theregister.com/2025/05/22/euro_cloud_body_ecco_says_broadcom_licensing_unfair/
[29] https://leitmotiv.digital/publications/breaking-the-cloud-monopoly

company Kyndryl[lxxxiv]. Solvinity offers cloud services to the IT company of the Dutch administration, including the back-end of digital wallet, used by 16.5 million Dutch citizens to verify their identities in order to get access to the tax administration and other departments. A non-European policy affecting the provision of Kyndryl's services in the EU would thus cause disruption for 90% of Dutch citizens. Threats to operational autonomy and of data access are particularly concerning in highly critical use cases relying on cloud and AI computing services[lxxxv]. For example, their use in healthcare, defence and certain public sector services often involves the processing of highly sensitive data. Service interruption in these sectors can have significant adverse effects on the EU economy and society. Some public sector actors are undertaking steps to limit exposure to such risks. For example, the Dutch parliament called on the government to reduce its reliance on US cloud services[lxxxvi], and France mandates sensitive data to be exclusively stored and processed using SecNumCloud certified services[30] provided either solely by EU providers or Joint Ventures between EU undertakings and US CSPs (see section 2.3.4). This issue was also recently illustrated by the postponement of Finland's electoral management system cloudification[31], previously awarded to AWS, and France's switch from US solutions to open source equivalents to serve public sector video conferencing needs[32]. The European Central Bank requires banks to use hybrid architectures and a multi-cloud approach[lxxxvii]. The US requires Federal Agencies to use only cloud services authorised under the Federal Risk and Authorization Management Program (FedRAMP)[33]. While dependence is widely considered as a critical risk to service continuity and operational autonomy, and demand for sovereign cloud solutions is growing[34], a coherent framework to address this challenge is still lacking at EU level.

Dependence on US providers also exposes EU user data to extraterritorial laws and potential US government access resulting from the US Clarifying Lawful Overseas Use of Data (CLOUD) Act[35] in the context of criminal proceedings, or Section 702 of the US Foreign Intelligence Surveillance Act[36]. Access can be granted unilaterally, without the involvement of EU judicial or public authorities. In a sworn testimony before the French Senate, a representative of Microsoft affirmed that the company could not guarantee that French data would not be transmitted to US authorities, even in the absence of explicit authorisation[lxxxviii]. Any data managed by a US-headquartered provider or its subsidiaries is potentially exposed, including sensitive business information, intellectual property, and personal data of EU citizens. Such exposure, especially of sensitive business or public data, can raise significant concerns when considering strategic entities, public authorities, and high-profile individuals. More generally, a lack of trust in cloud and AI computing services is slowing down European users' adoption of other digital services[lxxxix]. This lack of trust is also caused by technical aspects such as not having control over the supply chain,

[30] For instance, the platforms for electronic invoices shall be ISO/IEC 27001 certified and stored on one of the providers qualified by SecNumCloud: Facturation électronique et plateformes partenaires.

[31] See Finland's Ministry of Justice delays plans for cloud migration - DCD

[32] Souveraineté numérique : l'État généralise « Visio », sa solution de visioconférence sécurisée et souveraine à destination des agents publics – Presse – Ministère des Finances

[33] FedRAMP is an authorisation process for cloud services used by US federal agencies. Obtaining such authorisation is mandatory for all CSPs wishing to work with US federal agencies. It provides a standardised approach for the security assessment of cloud services in three impact levels (low, medium, high). In terms of European providers, three SAP products are authorised at level 'moderate' and the Accenture Insights Platform (originating in US, headquarters in Ireland) is authorised at level 'high'.

[34] 84% of European cloud users are already using or planning to use sovereign cloud solutions. See: How Digital Sovereignty Is Influencing Cloud Solution Choice

[35] The CLOUD Act facilitates the access of US law enforcement authorities to electronic data held by service providers that fall within US jurisdiction in the context of criminal proceedings. It affects providers of electronic communication services and remote computing services that are subject to the authority of US courts, either because they are established in the US or because they have a sufficient presence to be subject to US personal jurisdiction. When presented with a valid legal process, including a warrant for the content of communications meeting the high standards of probable cause, these entities can be obliged to disclose the contents of electronic communication and any related record or other information pertaining to their customers, regardless of whether the data are located within or outside of the US.

[36] FISA Section 702 permits the US government to conduct targeted surveillance of foreign persons located outside the US to acquire foreign intelligence information. Under Section 702, the US Attorney General and Director of National Intelligence may issue directives compelling US electronic communication service providers to provide such information, including via bulk data collection.

not being able to carry out audits and penetration testing, or the uncertainty of where the data is located[xc].

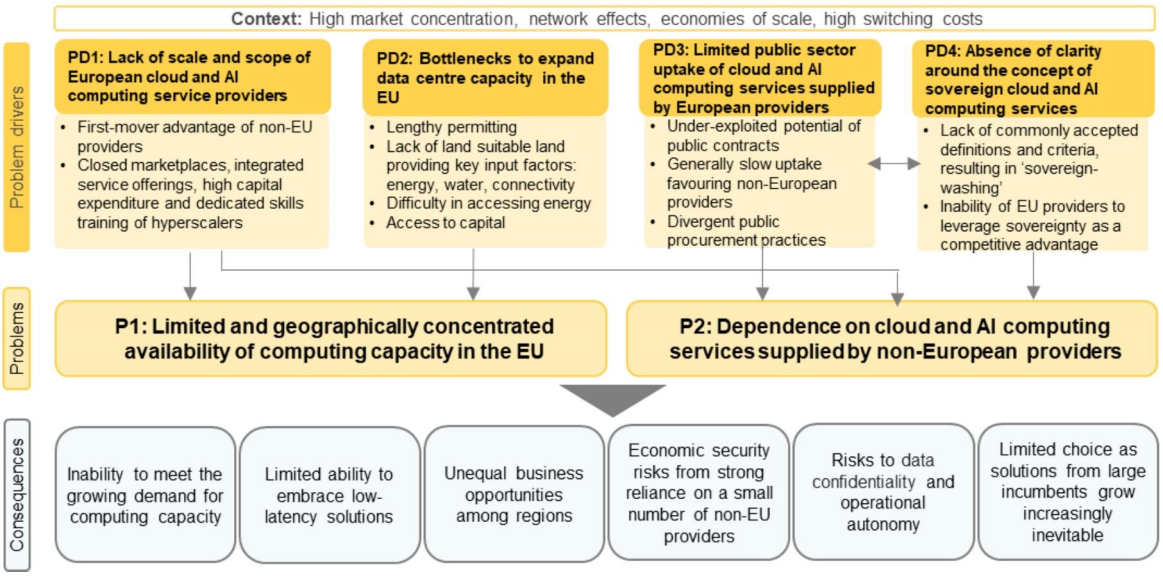
2.3. What are the problem drivers?

The two identified problems are closely interlinked, as they relate to consecutive stages of the same value chain, with a clear supply-demand relationship: cloud and AI computing services require adequate underlying infrastructure, while data centre investments rely on expected demand for such services. Problem 1 concerns the physical infrastructure layer, involving data centre operators, utilities, local authorities and investors. Problem 2 relates to the downstream market for cloud and AI computing services, characterised by distinct market structures, competitive dynamics and regulatory frameworks. Accordingly, the analysis of the root causes behind these two problems is presented separately, while acknowledging their interdependence. Four underlying drivers are identified: one specific to Problem 1, two specific to Problem 2 and one common driver that affects both problems.

Problem 1 relates to the limited and geographically concentrated distribution of compute capacity in the EU. It stems from two underlying factors: one related to market dynamics and the other to regulatory fragmentation. On the first one, first-mover advantage of non-EU providers reinforced by path dependency and network effects has led to market entry barriers that limit the scale and scope of EU cloud and AI computing service providers (PD1), thus hindering the deployment of capacity in the EU territory. As for the second factor, regulatory fragmentation and bottlenecks of a different nature have further slowed down the expansion of data centres (PD2), reducing international investors' interest, and thus contributing to the limited computing capacity, while also reinforcing geographical imbalances.

Problem 2 concerns the dependence on cloud and AI computing services supplied by non-European providers. Like problem 1, it is driven by the lack of scale and scope of EU cloud service providers (PD1), which makes reliance on non-European providers inevitable. The limited public sector uptake of cloud and AI computing services supplied by European providers (PD3), even in segments where local presence is essential, further hampers the creation of a large, unified demand for such services. This weakens EU providers' ability to invest, which results in foregone economic opportunities and deepens dependence. Finally, the absence of clarity around the concept of sovereign cloud and AI computing services (PD4) keeps European providers from commercially leveraging sovereignty as a distinguishing factor for themselves, further contributing to the problem.

Figure 4. Problem tree



2.3.1. Problem Driver 1 (PD1): Lack of scale and scope of European cloud and AI computing service providers

An important driver behind the limited and geographically concentrated availability of EU-native computing capacity and services is rooted in the comparatively small scale of European providers relative to global hyperscalers, as a result of the rapid development of the data centre and cloud sector in the EU. Notably between the years 2017 and 2021, this led to a significant market concentration around only a few non-European market incumbents well-placed to respond to the growing demand at scale which was out of reach for their European competitors.

As discussed under section 2.1, historically, the earlier cloud computing services were developed in the United States. Their early scale advantage reinforced their position as the world's leading data centre hub[xci], which US providers leveraged for global service provision. Hyperscalers invested aggressively in infrastructure, and building networks of data centres connected via submarine cables that enabled data flows into European markets[xcii]. This first-mover advantage reinforced their leadership in the continent, setting a ***high entry and growth barrier for European providers***.

Hyperscalers leveraged their scale to standardise services, invest in innovation and accumulate the financial resources to deploy compute capacity globally: today the AWS cloud spans 117 availability zones (AZs) within 37 geographical regions[xciii]. By comparison, OVHcloud has 37 AZs[xciv]. Due to their comparatively ***higher scale and financing advantages***[xcv], the ongoing expansion of data centre capacity in the EU is driven by non-European CSPs[xcvi]. As demand for local capacity grows, hyperscalers are able to secure land and grid access for their own data centres and (pre)lease large amounts of co-location data centre space, thus becoming anchor tenants for larger sites, while European CSPs struggle to access the same resources for developing digital infrastructure[xcvii] and are relegated to residual capacity under less attractive conditions. This is visible in the geography of Europe's data centres: the FLAPD hubs (Frankfurt, London, Amsterdam, Paris and Dublin) comprise over 60% of operational capacity and around half of the new and planned capacity is mainly driven by hyperscalers pre-leasing and committed projects[xcviii]. Scale and scope advantages of large providers reinforce the convenience of building in existing hubs.

Faced with these market dynamics, most European providers remain smaller, specialised and nationally fragmented, lacking the scale, scope or cross-border integration to deliver comparable cloud services. Comparatively lower revenues reduce their ability to invest in infrastructure expansion or innovation[xcix]. Google, for example, spent USD 9.6 bn on DCs across the globe in Q3 2025 only[c]. The capital expenditure of OVHCloud for the entire financial year 2025 amounts to EUR 361.4 m with EUR 51 m devoted to infrastructure and networks[ci]. Taken together, these factors (a) reinforce the structural advantage of large non-EU providers in securing key resources at scale, (b) further constrain the ability of European providers to expand, and (c) contribute to the current shortage and spatial concentration of computing capacity in a few established hubs, leaving significant areas of the Union under-served in terms of local compute.

The lack of scale and scope of European cloud and AI computing service providers is also closely linked to the second problem, i.e. the dependence on cloud and AI computing services supplied by non-European providers.

As mentioned under section 2.1, hyperscalers leverage bundles of services to operate as "walled gardens" meeting "all" customer needs, often within their own ***closed marketplaces***[cii]. The convenience of accessing all cloud-related services from a single provider is a key driver for customer choice[ciii]. AWS and Microsoft Azure each have 200+ services across their portfolios, and Google Cloud delivers 100+ specialised offerings available at their proprietary marketplaces. The absence of a comprehensive vendor-neutral marketplace creates an **imperfect information** environment about available services and their characteristics and negatively affect the

comparability of services across providers and general awareness of users about the services offered by smaller, including European, providers (discovery problem). End-users desire simplicity and have grown accustomed to one-stop shops delivering everything from Infrastructure-as-a-Service (IaaS) to Software-as-a-Service (SaaS) on a global scale, a level of integrated service that hyperscalers readily supply. Customers may therefore make suboptimal choices because they cannot easily compare offers. ***Imperfect information*** constitutes a failure in the market for cloud and AI computing services and reduces competitive pressure on incumbents.

Hyperscalers also offer dedicated professional training[37] and certification programmes[38], including through partnerships with key IT consultants and system integrators tailoring hyperscaler tools to specific customer needs[civ] that re-sell or promote their services[cv]. This has led to high transaction costs of leaving the hyperscalers ecosystems and a form of ***skills lock-in***[39].

Lock-in practices and the absence of technical interoperability further bolster the hyperscalers' market position by making it less likely for customers to switch to another provider[40]. In a market characterised by ***network effects*** and high switching costs[cvi], the initial choice of cloud and AI computing service provider limits future possibilities for diversification. This has posed high entry barriers for 'late' entrants, notably European ones[41]. Large providers leverage their strong position in the cloud market to attract customers with low entry prices, for example through cloud credits[42], but also to expand into the emerging market of AI computing services[cvii], through tying and bundling practices - linking together new AI applications with existing cloud products - and preferential access to computing power[cviii]. Their extensive service portfolio is also a competitive advantage for attracting AI companies as customers since they rely on the advanced offering of large providers to provide better usability.

European providers do not offer the same breadth of services. OVHcloud and Scaleway, for example, offer around 80 services[cix] whereas the US hyperscalers, such as Amazon, offer around 200. Annex 13 provides a comparative analysis of a sample of service of European vs American, demonstrating that EU providers usually cover well core IaaS and PaaS services but also highlight the actual gaps which tend to be more specific. These relate mainly to native AI/ML platforms, serverless, and integrated analytics pipelines where European providers have not yet reached hyperscaler maturity.

A smaller catalogue of services does not equate to lower quality, as argued later in this section. Gap analyses show that European providers offer equivalent quality in their services to those offered by the hyperscalers[43] but with rather a more ***limited integration***: To obtain access to a similar breadth of services as those offered by a single hyperscaler, a customer must combine

---

[37] During the COVID-19 pandemic, for example, AWS and Google Cloud offered free resources for training cloud skills and getting them certified: See here and here. AWS offers exam vouchers for certifying one's cloud skills to participants of EU-certified cloud courses for SME employees and jobseekers: Free EU-certified Cloud & Gen AI courses for SME employees and jobseekers — now open for enrolment! | Digital Skills & Jobs Platform.

[38] AWS for example reports 1.05m of individuals certified to their products. AWS Certification.

[39] See Ofcom's Cloud Services market study – October 2023. This structural dependence on non-EU proprietary solutions has also been cited by several SMEs as part of their Call for Evidence contribution.

[40] Competition authorities are increasingly scrutinising behaviours such as switching barriers of technical, contractual, and financial nature (including egress charges). Other relevant factors are a lack of standardisation and interoperability among services and the ability of large providers to attract customers through free credits and volume discounts. As discussed in section 1.2 and Annex 7, the Data Act creates a right for customers to switch and tackles relevant barriers.

[41] The entry barriers for EU providers are, for example, described in the Autorité de la Concurrence's opinion on competition in the cloud sector: Avis 23-A-08 du 29 juin 2023.

[42] Cloud credits are typically offered as short-term credits to attract new customers or motivate existing customers to adopt a new service or as long-term credits for selected customers, especially start-ups, to allow them to grow a cloud-native business in the environment of a given CSP. See: Report Covers. Ofcom has found that AWS offers up to $100k, Microsoft offers up to $150k, and Google offers up to $100k for each year over two years (so a total of $200k), as part of their credit programs for 'start-ups'. See: Cloud services market study final report.

[43] As discussed in this section, the simple fact of widespread uptake does not equate to a superior quality of services by non-European providers. Instead, the breadth and integrated nature of services is a major factor of distinction.

solutions from multiple providers[cx] – each requiring different skills[44], using different tooling, and employing different operational procedures. In the absence of tools that easily enable such combination of resources, such as cloud brokers[45], customers must invest their own resources to integrate services from different providers through custom developments.

A broader and a better integrated catalogue offers an advantage to US providers but this comes with a caveat. The latest Eurostat data shows that the services EU enterprises actually rely on most are email, office software, file storage, database hosting, and compute power[46], which are core IaaS workloads: virtual machines, managed databases, object storage, and nowadays also PaaS, with managed Kubernetes (orchestration). This points to the fact that customers seldom use a service catalogue to its full extent, something confirmed through interviews with European CIO public and private organisations, as well as by reports that find that only few customers use a large breadth of services from hyperscalers.[47]

Another factor for the low adoption of European offers is the limited visibility of said offers, as exemplified by market reports which rarely mention European providers[cxi]. All this places a high ***commercial barrier to greater uptake of European cloud and AI computing services***.

The hyperscalers' size also allows them to better overcome barriers for offering their services across the EU[48]. Consequently, European providers often focus on highly specialised market segments, such as the treatment of sensitive workloads requiring high-quality and secure services[cxii]. For example, the Polish provider CloudFerro supports space-related use cases such as the ESA Civil Security programme and CODE-DE, a German Copernicus Data and Exploitation Platform. Italy's leading provider Aruba provides the country's eID services. The general high quality of services is highlighted, for example, by the recognition of OVHCloud and Scaleway in Gartner's list of best Strategic Cloud Platform Services[cxiii]. Nevertheless, ***European CSPs are typically geared towards their home market***. For example, OVHcloud generates 48% of its revenues in France compared to 29% in other European countries and 26% in the rest of the world. Similarly, IONOS generated 56% of its revenue in 2024 in Germany, as compared to only 8% in Spain, 5% in France, and 3% in Poland as the next biggest markets in the EU[49]. This phenomenon is even more pronounced in the Italian market. 89.7% of Aruba customer base is in Italy, followed by only 0.6% in Spain and 0.5% in France[50]. In 2021, the European Alliance on Industrial Data, Edge and Cloud gathering all main European cloud providers pointed out their lack of ability to exploit the Single Market and offer their services across borders efficiently as one of the main barriers to scaling up and being able to compete with non-European providers[51]. This, paired with the absence of effective interoperability mechanisms across services or solutions that allow for a federation of cloud resources among CSPs, prevents European providers from achieving economies of scale (see also section 2.2.2).

Taking the considerations above, and under the same market conditions, ***US hyperscalers have been able to thrive in the EU while their local competitors have not***. The hyperscalers are able to exploit massive economies of scale, integrated ecosystems with default interoperability across services and high capital expenditure, which allow them to offer cheaper and broader services.

---

[44] SMEs have also pointed to workforce certifications being skewed towards non-EU vendors, thus reducing the possible adoption of European alternatives.

[45] A cloud broker is a 3rd-party that adds value to cloud services on behalf of cloud service consumers. It delivers: 1) aggregation from multiple cloud services (from possibly different providers) into a unified offering 2) arbitration, allowing switch among multiple providers dynamically based on e.g. cost 3) intermediation. Gartner, Alonso et al. "Federated Cloud Service Broker (FCSB): An Advanced Cloud Service Intermediator for Public Administrations" .

[46] See Eurostat

[47] See the blog post introducing the Civo 2024 report '*Has Cloud Computing lost its way to complexity and cost?*'

[48] Diverging national cloud cybersecurity certification schemes require providers to get certified several times.

[49] https://firmsworld.com/ionos-group-comprehensive-profile

[50] List of Aruba Cloud Customers

[51] European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf

Due to their global scale and capital, hyperscalers are able to spread compliance costs across the different national markets over a large revenue base, amortizing them across scale so the average compliance cost per unit of revenue (e.g. service) falls with scale. Conversely, European providers remain sub-scale and confined to niche segments, focused mainly on their own national markets and legal regimes. The services offered by EU providers, while equal in innovation and quality, are not as integrated as the services offered by the hyperscalers nor they benefit from a large ecosystem gravity, which prevents demand from pooling into contracts large enough to justify more investments. Due to the sub-scale, compliance costs for EU providers remain higher, which may slow them the release of advanced features that would allow them to meet the expectations of customers operating in certain critical markets.

The outcome is a ***Single Market failure***: in a genuinely unified market, all providers should be able to scale across borders with relatively uniform rules, standards, and buying channels, allowing efficient firms to grow and compete on equal footing. However, persistent regulatory and contractual heterogeneity and fragmentation (see also next sections), as well as siloed demand, mean that the EU's market remains de facto segmented, so network effects and economies of scale accrue disproportionately to already scaled non-EU incumbents rather than enabling EU-based providers to reach competitive size.

2.3.2. Problem Driver 2 (PD2): Bottlenecks slowing down data centre expansion

The second driver concerns bottlenecks and regulatory fragmentation, which have contributed to slowing the expansion of data centre deployment, reducing attractiveness of Europe for investors and as a result contributed to limited computing capacity and persistent geographic imbalances.

Companies seeking to build data centres in the EU are faced with a fragmented policy and regulatory environment[52]. For example, Germany's Energy Efficiency Act imposes Germany-specific obligations on data centres related to the use of renewable energy and heat recovery[53]. In the Netherlands, stricter rules are applied on new facilities in the Amsterdam region as opposed to other parts of the country[54]. In Poland, different permits are needed for different types of data centres[55]. Bulgarian zoning regulations altogether lack an adequate category for data centres. In the context of infrastructure buildout, the most relevant bottlenecks and frictions are found in permitting, availability of suitable land, grid access, and access to capital.

Permitting procedures for infrastructure development – which encompass zoning and land allocation, building permits, utilities and grid connection authorisations, and environmental permitting – involve multiple, often inconsistent layers of national and local regulations with multiple uncoordinated stakeholders and non-centralised processes. DCs are often not mentioned in national or municipal planning regulations, creating uncertainty and requiring additional rezoning processes in some jurisdictions[cxiv]. Permitting regimes typically ignore the strategic dimension of DCs for the EU economy, notably their enabling role for the EU uptake of digital solutions. Most jurisdictions require environmental review, ranging from basic assessments to full Environmental Impact Assessments that further lengthen the permitting process[cxv]. In most Member States, permitting involves repetitive requests and lengthy timelines, which can be aggravated by community opposition and appeals[56].

---

[52] For the complete analysis on the different regulations concerning data centre deployment in 12 MS, see Annex 4 section 9. See also here pp 19-20: 2025-Data-Center-Site-Selection-Dynamic-Brief.pdf

[53] Watson Farley & Williams (2024). Data centres: An international legal and regulatory perspective—Spotlight on Germany. Available at: https://www.wfw.com/articles/data-centres-an-international-legal-and-regulatory-perspective-spotlight-on-germany

[54] Royal HaskoningDHV (2023Navigating Dutch data centre challenges and opportunities. https://www.haskoning.com/en/newsroom/blogs/2023/navigating-dutch-data-centre-challenges-and-opportunities

[55] Dudkowiak, M. (2025). Data Center Investments in Poland | Law & Development Guide 2025. Dudkowiak Kopeć & Putyra. https://www.dudkowiak.com/invest-in-poland/data-centers-investments-in-poland/

[56] See as an example, the case of Apple in Athenry in Ireland.

The example of Germany illustrates well how and why permitting has emerged as a bottleneck for data centre deployment in light of the recent significant increase in demand for data centre capacity (see section 2.1.1). Germany's central location in Europe and its proximity to business users have made it a major data centre hub, despite comparatively long timelines for permitting. Early investments have resulted in strong path dependency and network effects, with new capacity continuing to cluster around established hubs despite rising congestion costs, grid limitations, and regulatory barriers. However, with demand for data centres growing, permitting is now a bottleneck holding back the fast expansion of data centre capacity that would be necessary to reduce the capacity gap. Illustrative cases in Ireland and Luxembourg show how administrative delays caused [57]data centre projects to be cancelled or delayed. In response, Member States or regions have adopted policies to accelerate DC deployment, for example by offering transparent planning procedures (Denmark), pre-designating areas (France), naming DC projects as of "strategic economic interest" (Spain at regional level), enabling parallel rather than sequential permitting (Germany), encouraging DCs to locate within existing industrial areas (Finland) or through tax incentives for DC operators (Sweden). While these acceleration measures facilitate short-term capacity expansion at national level, they contribute further to the regulatory fragmentation across the Single Market.

Another factor slowing down data centre expansion is ***land availability,*** the difficulty for DC operators to identify suitable sites. DC sites must display specific characteristics in terms of access to utilities (energy, water) and connectivity, making suitable real estate scarce. Connectivity is a particularly relevant pull factor for selecting appropriate sites for DC deployment[58], thus reinforcing concentration in existing hubs[cxvi]. Land scarcity is aggravated by large cloud service providers acquiring land and reserving energy capacity, without building DCs on the site[cxvii].

Energy availability. With respect to energy needs, different modelling approaches indicate that DC energy consumption is foreseen to grow at an average annual rate of 13% between 2023 and 2030, twice the 2018-2023 growth rate[cxviii]. Energy prices in Europe are two to three times higher than in the US and China, as shown in the table below, while they amount for 40-50% of DCs' operational costs, creating a competitive disadvantage for the EU[cxix].

Table 2. Industrial electricity prices (€/kWh – all data 2025, except China 2024)

US[59]	China[60]	EU-27[61]	Ireland	Germany	Italy	Sweden	Finland
€ 0.090	€ 0.081	€ 0.190	€ 0.296	€ 0.275	€ 0.271	€ 0.121	€ 0.101

Access to energy grid constitutes an important bottleneck in the construction of DCs[62]. In parts of Europe, grid constraints have resulted in moratoria on new DC connections, especially close to established hubs[cxx]. Connecting a DC to the grid can take between 3 and 10 years, depending on the Member State: around 3-5 years in emerging markets (Italy or Spain) and 7-10 years in established hubs (Frankfurt, Amsterdam, Paris or Dublin), with some projects experiencing delays of up to 13 years due to grid congestion[63cxxi]. In the case of brownfield sites where there is a

[57] Apple: see e.g., Guardian (2018), available (here) & Data Centre Dynamics (2022), available (here). Google: see e.g., Delano (2025), available (here) & RTL (2024), available (here).
[58] Access to connectivity was also mentioned as a key problem by most of the SMEs in the public consultation.
[59] Average Price of Electricity to Ultimate Customers by End-Use Sector, available here.
[60] China's Industrial Power Rates 2025: A Guide for Investors.
[61] Eurostat's non-household prices refer to the standard medium industrial band (annual consumption 500 to 1999 MWh) including all non-recoverable taxes and levies. These are widely used as an official benchmark for industrial power costs and for comparing Member States. Available here.
[62] This was also flagged by all the SMEs responding to the questionnaire as an important or highly important problem their organisation has encountered when expanding or building their infrastructure in the EU. SME also underlined that availability and affordability of (low carbon) energy, and of a utility provider's infrastructure nearby where the key factors that have driven their decision to select a DC's location.
[63] It is important to note that these delays are the result of grid congestion and limited availability. When it comes to grid connection, a 3 months deadline for receiving information on treatment of the connection request (i.e., the result of the permitting procedure) has been introduced by 2024 amendments to the Directive (EU) 2019/944.

previous power grid connection, this interval is highly reduced[cxxii], but these sites can be insufficient to meet the needs of large DC projects. To overcome grid interconnection delays, DC operators are increasingly considering producing their own energy, with a dedicated microgrid. In some cases, such energy production could be based on gas turbines[cxxiii], which would significantly increase their scope 1 greenhouse gas emissions[64].

Another bottleneck holding data centre expansion at the necessary speed is limited ***access to capital****:* over the past five years 58% of global DC investment occurred in the US with a record in 2023[cxxiv], with Europe accounting for a smaller share[cxxv]. AI computing infrastructure can be ten to thirty-times more expensive than general-purpose DCs[cxxvi], requiring massive capital investment. The EU's fragmented financing landscape lacks the depth of an integrated capital market. Compared to the US, the UK[cxxvii] and China[cxxviii], European investors have treated DCs as a niche market rather than a distinct asset[cxxix]. In addition, many parameters affect the bankability of DC projects[65] such as the size of the operator, permitting and access to grid. Combined with Europe's fragmented capital markets[66] and the high risk associated with smaller EU CSPs, notably outside the FLAPD markets, these challenges slow down capital mobilisation for DCs.

In parallel to these bottlenecks across EU markets, water availability can be a critical factor for DC deployment for DCs that use cooling technologies which rely on water. With evaporative cooling techniques, a 1-megawatt DC can use up to 25.5 m litres of water annually[cxxx], a potential issue in water-stressed locations[cxxxi]. While this is not a systematic investment bottleneck in Europe compared with other constraints[67], its importance in site selection and environmental assessments highlights the need to consider water risk as a relevant aspect of future infrastructure planning.

In responding to this unprecedented demand growth, the factors highlighted above are holding the EU back from swiftly building the computing capacity needed to respond to the increase in demand, including for socially valuable infrastructure. The identified bottlenecks have historically not weighed as heavily as today: the demand for data centres has surged with the growing role of digital services and, more recently, with the advent of AI, which also require data centres located closer to users. This results not only in a capacity gap but also in the reinforcement of geographic imbalances, driven by regulatory fragmentation and the risk of regulatory arbitrage. This driver can be considered a ***coordination failure*** among investors, energy system operators, and public authorities, coupled with ***regulatory failures*****,** as a result of fragmented practices and divergent regulations. The first hinders effective communication of where new capacity could yield the greatest net benefits, while individual regulations have created obstacles to the proper functioning of the internal market, increasing compliance costs and preventing the cross-border scaling for smaller operators. Even though larger companies face the same rules, they are able to internalise such costs and regulatory heterogeneity given their global scale.

2.3.3. Problem Driver 3 (PD3): Limited public sector uptake of cloud and AI computing services supplied by European providers and diverging procurement practices

This driver is innately linked to PD1. While some analysts[cxxxii] argue that the dependence on non-European cloud and AI computing services stems from the limited scale and scope of these

[64] Today's DC scope 1 emissions are largely limited to diesel back-up generators which typically operate only a few days per year for testing.
[65] In the public consultation, most SMEs flagged having difficulties in getting funding to develop capacities. Among the respondents to follow-up questions, several flagged access to finance and/or high interest rates when procuring next generation GPUs as a key limitation to expand capacity. On accessing finance, SMEs frequently underlined difficulties in accessing capital, such as loans or equity.
[66] EU capital markets remain fragmented along national lines. The absence of a pan-European financing framework with common legal structures, or cross-border Real Estate Investment Trusts regimes underpin the difficulties of raising capital quickly.
[67] Alternative cooling technologies can be used (often at the expense of a lesser energy efficiency).

services (PD1), others argue that the scale and scope of these services can only grow based on stable anchor customers[cxxxiii].

As discussed in relation to PD1, the initial growth of today's largest cloud and AI computing service providers was fuelled by public contracts. Similar opportunities did not emerge for European providers. Generally, public sector cloud uptake and corresponding spending on cloud and AI computing services is relatively low. Looking at 2024 publicly available data from the portal of Tenders Electronic Daily, approximately 3.13% of ICT awards were dedicated to cloud and AI computing services. Out of all award notices published on the portal in 2024, 0.34% were related to cloud and AI computing services. Budgetary constraints and a shortage of a digitally skilled workforce to build their own private cloud constructs[68] make public authorities dependent on cloud and AI computing services from external providers[cxxxiv]. The systematic uptake of cloud and AI computing services by the public sector is still a relatively recent phenomenon. For example, Italy only set up its Polo Strategico Nazionale to provide public administrations with access to cloud infrastructure in 2022[cxxxv] and Germany launched its government cloud in March 2025[cxxxvi]. While all Member States have developed national AI strategies and 21 of them have in place dedicated cloud policies, Member States vary widely in terms of maturity in the uptake of cloud services or in how they allocate and report public funding associated with these initiatives[69]. In some Member States, public procurement practices impede the procurement of pay-per-use cloud and AI computing services as they cater more towards fixed-price contracts[cxxxvii]. Beyond pricing modalities, the ***lack of harmonised approaches to procuring cloud and AI computing services*** creates difficulties in developing and evaluating call for tenders[70]. Moreover, the approach to using cloud and AI computing services laid down in cloud strategies and policies varies significantly, even within the same public entity and does not always include risk assessments[71]. Where they do purchase cloud and AI computing services, an increasing number of public sector entities relies on services provided by non-European companies[72], sometimes concluding direct partnerships[73]. For example, Finland's State Treasury uses Oracle and Microsoft Azure, Denmark's state public services use OpenStack's private cloud, Belgium's public authorities use a hybrid G-cloud, which runs on the clouds by IBM, Microsoft and Oracle, and the Dutch Tax Office uses Microsoft Azure[cxxxviii]. Similarly, the Flemish government recently partnered with Microsoft[cxxxix]. Some public tenders directly refer to services from leading cloud and AI computing service providers[74]. A 2026 study by FOTI, the Future of Technology Institute, shows the pervasiveness of non-European providers also in the defence sector[75]. This results in foregone economic opportunities for European CSPs and closes off one avenue for obtaining the stable public contracts that have allowed US CSPs to scale (see PD1).

---

[68] Public authorities' ability to develop and operate cloud and AI solutions in-house is also often hampered by lower salaries in the public sector. Regarding limited ability to attract talent, see for example Strengthening the attractiveness of the public service in France – OECD – 2023, or the struggle by Italian data protection authority to recruit AI experts. Regarding budgetary constraints, see for example Data foundations for government: From AI ambition to action – Capgemini – 2025, where 66% public sector respondents report limited budgets for on-premise solutions as a factor limiting widespread adoption of Generative AI.

[69] OECD, 2025, Progress in Implementing the European Union Coordinated Plan on Artificial Intelligence (Volume 1) (EN)

[70] SMEs responses to the Call for Evidence have highlighted how public tenders tend to be designed for non-EU incumbents with scarce consideration for European SMEs.

[71] For the case of the Central government of the Netherlands, this is highlighted in a recent report by the Netherlands Court of Audit: Dutch central government in the cloud | Netherlands Court of Audit. Similarly, the 2022 EDPB Coordinated Enforcement Action on the Use of cloud-based services by the public sector reports that only 1/3 of the services procured by the Member States involved was subject to the necessary Data Protection Impact Assessment.

[72] For example, the Netherlands' Court of Audit has found that out of 1588 cloud services audited, more than half were procured from AWS, Microsoft and Google. See also: Trotz Abhängigkeit und Datenschutzrisiken: Behörden gehen in die Microsoft-Cloud | Heise Online.

[73] See for example the recent announcement of the State of Bavaria: Vertrag soll bis Jahresende stehen: Bayern will in die Microsoft-Cloud | heise online.

[74] See for example this tender for the provision of cloud services from the portfolio of the cloud provider AWS by an authorised cloud reseller: Bereitstellung von Cloud-Services für den Betrieb der Förderzentrale Deutschland (FZD) | BMWE.

[75] Cloud Defence: an exposed European flank

While the described barriers to public sector cloud adoption affect public sector demand for all service providers, they have particularly pronounced effects on comparatively smaller European providers which do not have the resources to navigate diverging approaches to public procurement, and that prevent them from the benefits of the Single Market **(regulatory failure).** Moreover, budgetary and human resources constraints[76] as well as a lack of awareness for alternative solutions drive the public sector towards the purchasing of integrated service packages from large incumbents[cxl] (see PD1). At the same time, public sector organisations voice strong concerns related to the possible loss of operational autonomy and control over the data and associated infrastructure[77]. Different national approaches have emerged to identify what constitutes a sovereign cloud provider and leveraging public procurement, as evidenced for example by the recent Franco-German sovereignty task force[78]. Similarly, there are multiple and diverging national cybersecurity certification schemes, as described in section 2.2.1 of the report, with some of them integrating a sovereignty dimension, demonstrating a clear fragmentation in the internal market **(*systemic failure – fragmentation of the internal market*).** While potentially effective in pursuing individual Member States' policy objectives with respect to their enhanced autonomy, different national efforts come at the cost of increased regulatory fragmentation. This undermines the ability of comparatively smaller providers to easily navigate the European cloud market and offer their services across borders, including to public procurers. As discussed in the Draghi report, *"multiple different national rules in public procurement generate high ongoing costs for cloud providers. The net effect of this burden of regulation is that only larger companies – which are often non-EU based – have the financial capacity and incentive to bear the costs of complying*[79]."

This limited public sector uptake of cloud and AI computing services has spillover effects on the modernisation of public services. The adoption of cloud and AI is also a driver of public sector modernisation, as it enables administrations to move away from often fragmented, legacy IT systems toward more flexible, scalable, and interoperable digital infrastructures. By leveraging cloud and AI, public authorities can deploy new applications faster, improve service reliability, and respond more effectively to changing policy needs or crises. They also facilitate data sharing across departments and levels of government, supporting more integrated and user-centric public services. In addition, they reduces the burden of maintaining on-premises infrastructure, allowing resources to be redirected towards core missions. Overall, cloud and AI adoption underpins a shift toward a more agile, efficient, and digitally capable public administration.

Finally, cloud and AI-savvy public authorities are increasingly embracing OSS[cxli], thanks to its overall lower total cost of ownership but their benefits remain to be scaled. While OSS deployed on EU-based data centres addresses some concerns over confidentiality of data and enables custom-built solutions, it entails some difficulties regarding time, skills and lack of easily re-usable public procurement award criteria **(*regulatory failure – administrative burden*)**. This is exacerbated by public authorities lacking a common approach to open source, notably when agreeing to coordinated developments[80], or to the sharing and maintenance of existing code[81].

---

[76] The 2023 Opinion 23-A-08 of the French Autorité de la Concurrence on competition in the cloud sector points to a decline in organisations' overall in-house IT skills, due to higher reliance on managed services provided by private operators, which allow for savings but affect negatively such organisations strength of negotiation, choice and mastery of IT tools.

[77] 64% of public sector organizations surveyed as part of the 2025 Capgemini Data foundations for government: From AI ambition to action study express concern about data sovereignty, 58% about cloud sovereignty, and 52% about AI sovereignty as a factor in deciding about future technology choices.

[78] https://uk.diplomatie.gouv.fr/en/summit-european-digital-sovereignty-delivers-landmark-commitments

[79] 97e481fd-2dc3-412d-be4c-f152a8232961_en, p. 13.

[80] Several Member States (IT, FR) require a comparative analysis of existing open source and commercial solutions and mandate that applications developed for public administrations be released in open, public repositories. Others take a more voluntary approach (CZ).

[81] When public authorities release OSS, the maintenance and further development often end up depending on just one or two main contributors, undermining resilience and innovation. See for instance the log4J case where there was only one active member contributing to a library largely used to log actions in IT systems.

Additionally, many of the open source components widely used in today's services and applications are maintained by single individuals and small teams, creating critical points of failure (see the log4j case, mostly maintained by one individual and which is considered the second most commonly exploited vulnerability[cxlii]). Thus, while open source offers more transparency by releasing code openly for more eyes to review and faster bug discovery, it requires constant and expert monitoring to avoid that vulnerabilities are exploited by malicious actors.

2.3.4. Problem Driver 4 (PD4): Absence of clarity around the concept of sovereign cloud and AI computing services

In the absence of an agreed definition and criteria to evaluate sovereignty, users are left without the necessary information to assess whether a service is sovereign or not. At the same time, providers are left without a reliable opportunity to distinguish themselves commercially.

'Sovereignty' is often used in the ICT domain without a commonly accepted definition. Literature defines it as "*possessing the ability and competences to have reliable access to a technology it deems critical for its own system, without any structural, uncontrollable dependency from third countries*"[cxliii]. Currently, non-European service providers, including US-based CSPs, are at the forefront of offering sovereign-branded solutions for the EU market based on diverse characteristics. For example, AWS European Sovereign Cloud guarantees data residency in Europe with physical and logical separation from other regions and operation entirely run by EU residents[cxliv]. Oracle's EU Sovereign Cloud locates customer support, DC support, and DC operations fully in the EU and ensures management by a dedicated EU entity[cxlv]. An alternative approach takes the form of joint ventures, such as Bleu (partnership between Capgemini and Orange offering Microsoft services)[cxlvi] or Clarence (joint venture between Proximus and LuxConnect based on Google technology)[cxlvii].

The price of sovereign cloud offers over traditional ones is subject to diverse points of view, something not surprising given their recent arrival to the market. An analysis carried out by BCG[82] estimates that listed prices are 10% to 30% higher compared to the public cloud. According to BCG, "*Google Sovereign Cloud is priced 10% to 20% over the public cloud, while Oracle EU Sovereign Cloud charges a 15% to 30% price premium",* whereas *"Microsoft Azure Government carries a 15% to 25% price premium".* An empirical comparison of AWS pricing between the sovereign cloud offers and the eu-central-1 region (Frankfurt) of 6 AWS cloud services in January 2026 using AWS' provided calculator shows that the average price premium for the previously mentioned sovereign services is of 15%[83]. Against these observations, European service providers, possibly because sovereignty in the EU is easier for them to reach, declare in bilateral interviews that their prices should not be affected by sovereignty requirements and could even be lower than non-EU non-sovereign services. Real observed prices in actual competitive tenders, to which this assessment had access in confidence, show price differences ranging from +12% to -10% for the same level of sovereign service.

This can also be observed for "sovereign AI": For example, Oracle advertises AI solutions running on its sovereign cloud as "sovereign AI"[cxlviii], and OpenAI announced agreements with Germany as well as the UK Ministry of Justice, on the expansion of UK sovereign AI capabilities[cxlix]. The descriptions of these offers often also refer to high levels of cybersecurity. However, a technically cybersecure service may still be exposed to non-EU laws requiring the provider to grant data access to third-country authorities or to third-country policies intended to

[82] See BCG Cloud Cover: Price Swings, Sovereignty Demands, and Wasted Resources

[83] These are S3, FSX Windows, EC2, Lambda, RDS for PostgreSQL and DynamoDB. See: AWS European Sovereign Cloud (ESC) – Launch, Pricing, and What's Next

limit service supply. Moreover, the processing of data in the EU does not in itself prevent the control over the software by a non-EU entity[84].

The above-mentioned sovereignty claims are currently made without demonstrating the safeguarding of operational autonomy and the protection of data against foreign interference or access (see section 2.2.2). This ***imperfect information*** environment implies a failure in today's market for cloud and AI computing services leading to an ***information asymmetry*** as users do not have a reliable means of verifying whether a service is truly sovereign or not[85]. At Member State level, existing schemes on cloud cybersecurity certification sometimes contain a sovereignty dimension. For example, the French SecNumCloud aims to ensure the 'sovereignty of CSPs' based on strict technical cybersecurity requirements and non-technical – sovereignty - criteria. The adoption of SecNumCloud by cloud services remains rather low, and most European customers are unaware of the benefits in the services provided by European CSPs, despite an increased use of the notion of sovereignty to market their offers[cl].However, in the absence of clarity around the concept, this has not yet translated into meaningful commercial advancements[cli].

Thus, the lack of such a clear common understanding and enforceable criteria for sovereignty along with the solutions adopted by different Member States is resulting in further **fragmentation of the Single Market**. Announcements such as AWS investment of EUR 7.8 bn in an EU sovereign cloud[clii] indicate that today's incumbents are likely to capture the nascent market for sovereign cloud and AI computing services. In the absence of clarity on what constitutes a sovereign service, the definition will *de facto* be set by today's leading providers in a way that further enshrines today's dependence.

2.4. How likely is the problem to persist?

The problems can be expected to become increasingly acute. Despite continued investment in DCs, the gap between supply and demand of computing capacity will likely grow. The current timeline for DC deployment is likely to remain complex as rising demand puts additional strain on the already lengthy permitting processes.

Member States' national policies to attract DCs and accelerate their deployment will likely persist, complexifying the European market for operators and creating geographical imbalances regarding the deployment of DCs towards certain regions. Considering the importance of low latency, this will lead to unequal opportunities for businesses across the EU, notably in central and southern Europe where latency performance can fall short of AI or IoT solutions execution requirements[cliii]. Ultimately, insufficient access to computing capacity will limit businesses' ability to integrate AI into their operations, negatively affecting their competitiveness[cliv].

While lowering operating costs will incentivise DC operators to adopt energy efficient technologies, the industry's demand for energy will continue to grow. Without strategic energy planning and a focus on sustainable infrastructures, DC expansion will particularly challenge existing DC hubs and regions with high strain on natural resources, at the risk of crowding out electrification objectives in other sectors and generating increasing public opposition[clv]. The ongoing revision of the infrastructure planning under the TEN-E Regulation (2022/869) has a potential to reduce the scale of the problem.

---

[84] Delos Cloud (an SAP subsidiary operating based on Microsoft software for use by public administrations), for example, is deemed by the Interior Ministry of the State of Baden-Württemberg to not be fully sovereign beyond its infrastructure. As the application layer remains Microsoft software, the Ministry cautions that the software and data processed remains subject to the requirements of the US CLOUD Act, giving rise to data access without the customer's awareness.

[85] This has given rise to the term 'sovereignty washing', see for example: Sovereignty Washing - When 'Sovereign Cloud' Isn't Really Sovereign – VSHN AG. Similarly, SMEs respondents to the Public Consultation have stressed that foreign-controlled firms market services as "European" despite extra-territorial dependencies.

Considering these factors, the expansion of DCs in the EU will continue, but at a slower pace than needed to meet growing demands. This will continue to raise prices, a trend already noticeable for colocation and access to GPU capacity in Europe[clvi]. This shortage of suitable computing capacity may even lead EU businesses to move overseas[clvii] or delay the deployment of low-latency services to the detriment of EU's economic growth. Consequently, the provision of cloud and AI computing services to EU customers will continue relying on infrastructure located outside of the EU. Given the preference of many users for keeping their data in the EU, this bottleneck will slow down the adoption of cloud and AI computing services in the EU.

Today's stable market share of 15% for European CSPs shows no indication of change, despite a growing market[clviii]. The largest European CSPs may be able to solidify their position as national players, but their smaller customer base will hinder their capacity to invest, scale up and innovate. Conversely, hyperscalers will continue to innovate and grow into the AI market, with their solutions becoming indispensable, particularly for startups and SMEs and in MS where European CSPs lack a commercial presence. Current trends suggest that US dominance in development and adoption of AI technologies, with China catching up, will persist[clix]. European businesses and public authorities will continue to rely on US AI providers to the detriment of European service providers struggling to work at the frontier.

Dependence on hyperscale cloud and AI computing service providers, particularly for highly critical use cases, will continue to expose data to third-country access and carry risks to service continuity, endangering operational autonomy.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

Article 114 of the Treaty on the Functioning of the European Union (TFEU) empowers the EU to adopt measures aimed at improving the functioning of the internal market through the approximation of the provisions laid down by law, regulation or administrative action in Member States. These measures can take the form of a Regulation or a Directive. National approaches to expanding DC capacity risk creating a fragmented landscape on DC deployment and potentially a regulatory race to the bottom in sustainability and permitting requirements. Diverging public procurement practices for cloud and AI computing services and diverging sovereignty criteria may prevent providers from fully benefitting of the internal market. If EU intervention takes the form of a legislative proposal, it can be based on Article 114 TFEU.

Article 173(3) TFEU is the basis for enhancing the EU's competitiveness and innovation capacity. It enables measures to accelerate industry's adaptation to structural changes; encourage an environment favourable to initiatives and to the development of undertakings throughout the EU, particularly small and medium-sized undertakings and favourable to cooperation between undertakings; and foster better exploitation of the industrial potential of policies of innovation, research and technological development. The lack of computing capacity in the EU negatively affects the competitiveness of industry, keeping it from leveraging the full potential of adopting AI, particularly those that rely on low latency. By increasing the availability of compute capacity, this initiative aims to strengthen Europe's competitiveness and innovation capacity. If it takes the form of a legislative proposal, it can thus also be based on Article 173(3) TFEU.

Should the legislative proposal include elements associated with both improving the functioning of the internal market as well as addressing the competitiveness of the Union's industry, the proposal would take form of a single act, building on the legal basis provided for under Articles 114 and 173(1) TFEU, to ensure a coherent approach to address, in different ways, the need for strengthening of the Union's cloud and AI ecosystem.

3.2. Subsidiarity: Necessity of EU action

Article 5(3) TFEU stipulates that action at EU level should be taken only when the envisaged objectives cannot be sufficiently achieved by Member States alone and, due to the scale or effects of the proposed action, can be better achieved at EU level.

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

Closing this capacity gap and allowing European businesses and public administrations to leverage compute capacity while ensuring sustainability requires action at EU level. The dependence on cloud and AI computing services supplied by non-European providers has the same root causes across the EU and affects businesses and public administrations in all Member States. European service providers face difficulties to scale up across the EU, for example due to different national trustworthiness standards, particularly in public procurement. Divergent national procurement practices complexify the market for European providers and the underlying situation of imperfect information is a market failure requiring an EU-level response. Calls for EU-action to address these challenges were also made in the public consultation[86].

3.3. Subsidiarity: Added value of EU action

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

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

[86] In replying to this topic, 80% of respondents emphasised the importance of the EU reducing its reliance on non-EU cloud and AI computing service providers. Public authorities strongly supported coordinated EU-level action with 80% supporting EU-level actions such the establishment of cybersecurity guidelines; the adoption of standards, open specifications, and mechanisms to ensure interoperability; the creation of a mechanism to federate cloud and AI computing services across public administration within and across MS, the creation of guidelines with standard criteria to procure cloud and AI computing services and guidelines with standard award criteria. In addition, 72% supported the creation of clear environmental compliance requirement et EU level, and 66% were in favour of unified guidelines at EU level for energy efficiency for computing infrastructure. Finally, public authorities called for an EU-level definition of cloud sovereignty.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

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

4.2. Specific objectives

Specific objective 1 (SO1): Increase computing capacity deployed in the EU through innovative and sustainable technologies. By 2030, the EU should at least triple its current DC capacity, prioritising energy-efficient technologies in at least 80% of new installations. As demand continues growing, this should be considered an intermediate objective so that by 2035, the computing capacity in the EU should meet its needs.

Specific objective 2 (SO2): Ensure attractive conditions for the deployment of sustainable and innovative computing capacity[87]. While SO1 is aimed at the deployment of capacity, this SO targets the conditions for investment and deployment. By 2030, operators should be able to obtain all permits to build and run a DC in less than 18 months throughout the EU, including access to land, permits for energy access, and connectivity – which are also a major attention point for investors.

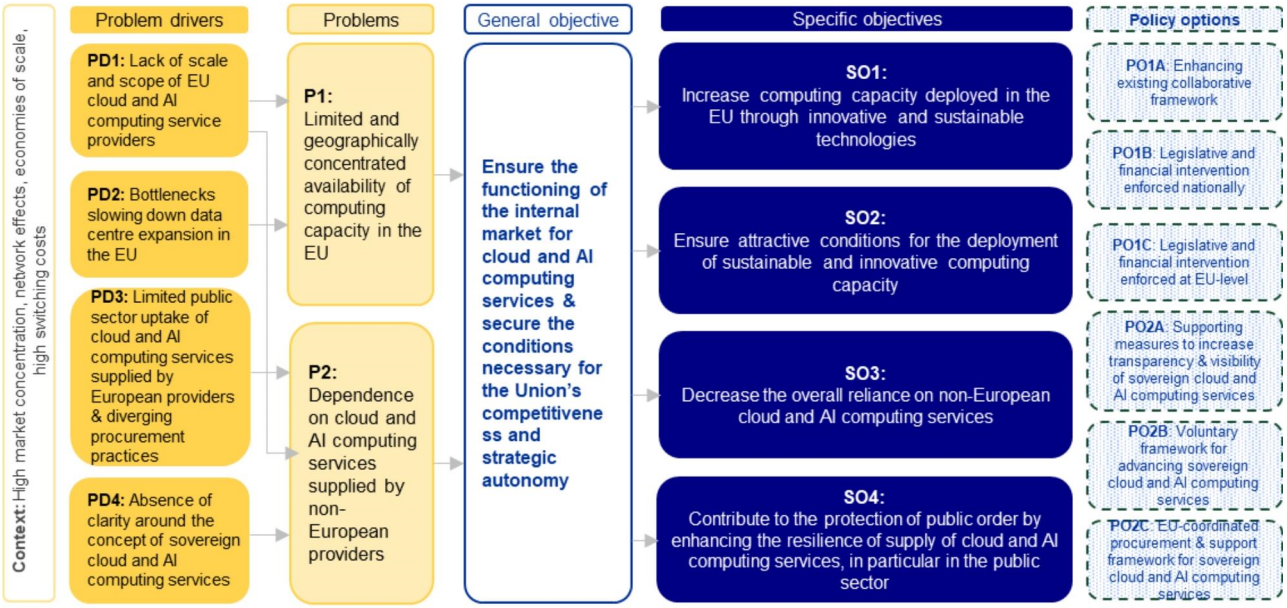
Specific objective 3 (SO3): Decrease the overall reliance on non-European cloud and AI computing services. By 2035, this intervention should increase the market share of European cloud and AI computing service providers in the European market to 30%. Strengthening the Union's strategic autonomy requires reducing dependencies and ensuring that European users have credible European alternatives to non-European incumbents. A stronger European supply base improves the Union's capacity to act autonomously and enhances long-term resilience, competitiveness, and security of supply.

Specific objective 4 (SO4): Contribute to the protection of public order by enhancing the resilience of supply of cloud and AI computing services, in particular in the public sector. By 2035, 100% of the highly critical use cases in the public sector should be operated using sovereign cloud and AI computing services to ensure data confidentiality, operational autonomy and prevent harms that could undermine public order. Highly critical use cases are those of a particular systemic importance and that underpin essential functions or involve the processing of sensitive data. Ensuring that, for them, data is protected**,** and service continuity is guaranteed is a key element of attaining strategic autonomy. That is why these use cases are a priority for the move towards services whose provision is outside of the reach of third-country policies that could result in data access or interruptions to service continuity, i.e. sovereign services[88].

Figure 5. Illustrative summary of the problems, drivers and objectives associated with this initiative

[87] An example would be a data centre using immersion cooling. This technology involves submerging servers in a non-conductive liquid, which is more efficient at dissipating heat than traditional air cooling. This approach not only reduces cooling energy consumption but also allows for higher server densities, making data centres more compact and efficient, generating more computing power while occupying less space and using fewer resources.

[88] Defining what constitutes a sovereign service is part of this initiative. However, already at this stage of the assessment, it is important to point out that sovereignty should not be equated with 'European'.



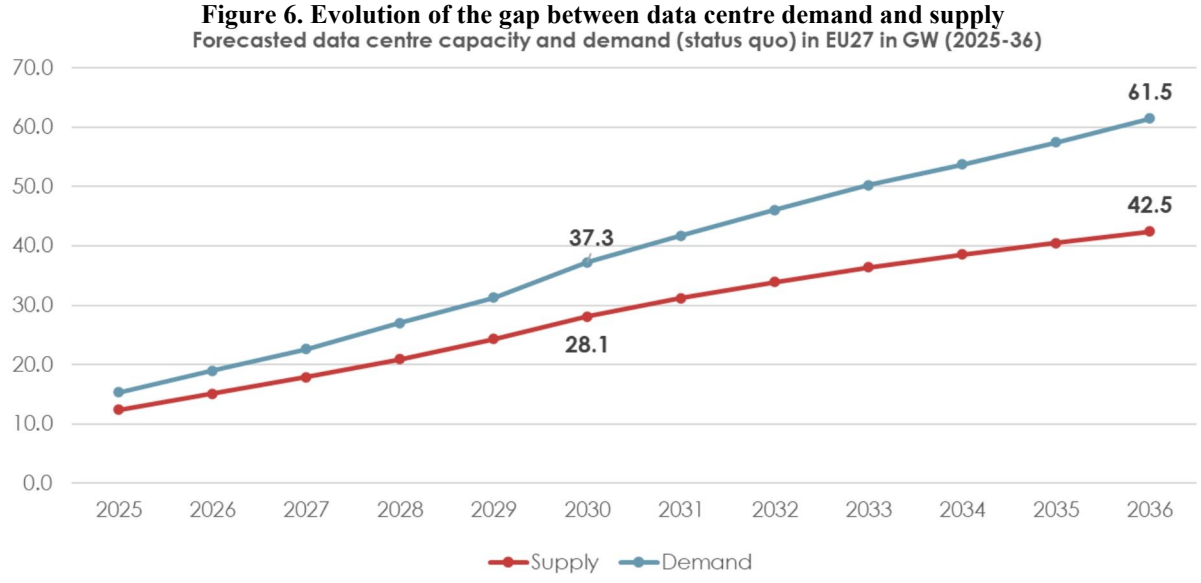
5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

The baseline scenario assumes that today's policies and regulations continue. Annex 9 presents the underlying assumptions.

For the limited availability of computing capacity in the EU (P1), the baseline scenario considers the projection of EU DC capacity in the absence of additional intervention in the period 2025-2036. Growth in the EU's total installed compute capacity, measured in DC IT load, is projected to reach around 42 GW by 2036, growing yearly by 12% over this period, yet demand for computing capacity is expected to increase by 13% over the same period, creating a structural capacity gap of 19 GW as seen in Figure 6 below, across all capacity growth scenarios[89].

Figure 6. Evolution of the gap between data centre demand and supply

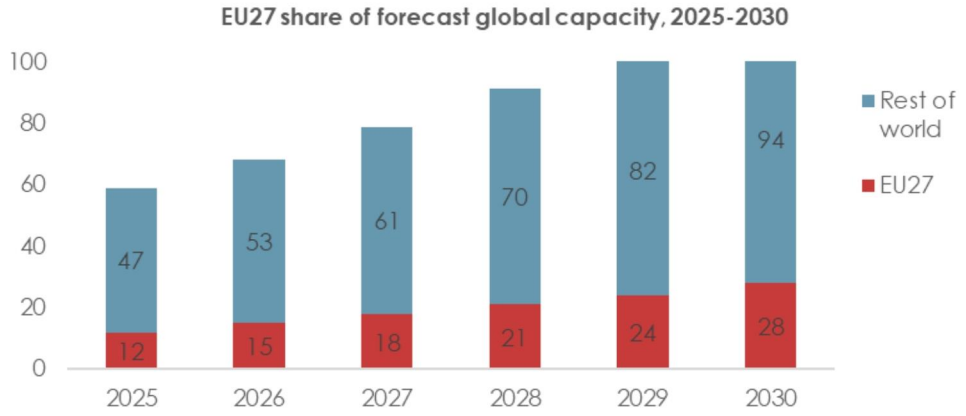


Source: Technopolis et al. (2025)[clx]

[89] The study presents projections for data centre capacity and demand across the EU27 based on three scenarios (low, central, and high). These projections illustrate the potential evolution of installed capacity and needs over the next decade, reflecting variations in natural resources, demand drivers, technological innovation, and market responsiveness. The study finds a structural capacity gap across all the different growth scenarios tested for this assessment, i.e. of 12 GW in the low growth scenario, 19 GW in the central scenario (used as the baseline) and of 23 GW in the high growth scenario. Please see Annex 4, Section 2.3 for additional information.

DC acceleration policies and regulatory framework remain non-harmonised across Europe. Some Member States would develop national strategies to make specific locations more attractive for DC operators. Outside of these possible strategies, bottlenecks such as lengthy permitting processes would persist and capacity expansion is expected to follow existing market trends, i.e. concentrated around existing hubs. Permitting delays, grid-connection queues and land-use restrictions would persist, with localised alleviation through national reforms. The Commission would continue pursuing greater transparency on the environmental performance of DC, notably under the EED and the upcoming review of the Taxonomy for Sustainable Finance. Industry may set additional sustainability targets, e.g. under the Climate Neutral Data Centre Pact. Electricity grid constraints would become a binding factor in several Member States by the early 2030s as total DC demand surpasses 200 TWh. Under current conditions, the International Energy Agency has estimated that around 20 % of announced projects worldwide are expected to experience significant delay or downsizing[clxi]. Public investment would remain focused on high-performance compute infrastructure for the training of large AI models (AI Factories, Gigafactories). Under policy option 0, the EU's compute supply increases in absolute terms but lags well behind other regions, as shown in Figure 7 below. North America and Asia-Pacific expand faster, increasing their share of global compute. This trend risks constraining AI model training and cloud workloads within the EU, particularly for SMEs and public sector users.

Figure 7. Forecast of data centre capacity in the EU-27 vs ROW from 2025 to 2030



Source: Technopolis et al. (2025)[clxii]

For the dependence on cloud and AI computing services supplied by non-European providers (P2), the baseline scenario considers that the market share of European service providers (15%) will remain stable despite the opportunities that a growing market can offer. The Policy 0 scenario reflects continued efforts under the Data Act to ensure cloud switching or parallel use of several providers. Given the recent adoption of the Data Act, its full effects will take time to materialise. The standard clauses recommended will allow for an easier switching of cloud services, whose consequences will be observable as they are progressively adopted. For the interoperability aspects, the effects are expected to take longer to materialize given the low number of existing open specifications and harmonized standards addressing the issue, that would become of mandatory application for providers following the mechanisms envisioned in the Act. The Data Act empowers the Commission to further standardization requestions and the adoption of open specifications compliant with the Data Act and that are published at a later stage. Pursuant to the recently launched investigation, a potential designation of large CSPs as gatekeepers under the Digital Markets Act may further open the market[clxiii]. The revision of the CSA could enhance the security and resilience of ICT supply chains including for cloud and AI computing services. The IPCEI-CIS will continue to support the participating European providers in the development of a multi-tenant cloud-to-edge software paradigm. The activities of the European Alliance on Industrial Data, Edge and Cloud will continue to enhance cooperation among European providers.

The Commission would pursue investment in OSS, such as Simpl, or the Open Internet Stack. While these may positively affect the uptake of cloud and AI computing services, they should be balanced against the problems and drivers spelled out in section 2. Without a common understanding of what a sovereign service entails, providers can promise a sovereign service to customers without clarity on its substance. This could lead to continuous uncertainty for service providers and users, particularly in the public sector. The absence of an EU-level cloud cybersecurity certification scheme is already resulting in national approaches, fragmenting the internal market. Finally, the ongoing parallel work on the Capital Markets Union strategy should address the question of availability of private capital more structurally. Against this backdrop, the baseline considers three scenarios of how the market share and revenues of European service providers will evolve in the period 2025 - 2036 without additional measures:

Table 3. Baseline scenario for Problem 2

Scenario	*Market share of EU providers in 2036*	*Cumulative revenues of EU providers (2025 – 2036) (EUR bn)*	*Cumulative revenues of non-EU providers (2025 – 2036) (EUR bn)*
Baseline (pessimistic scenario)	10%	438	33 212
Baseline (flat-share scenario)	15%	564	31 956
Baseline (optimistic scenario)	17%	611	31.483

The 15% baseline assumes European cloud providers maintain their current market share through a combination of modest revenue growth from rising customer interest in sovereignty and specialized use cases, offset by persistent structural barriers including vendor lock-in effects, hyperscaler bundling strategies, and the integration challenges that prevent easy switching. The 10% pessimistic scenario reflects the resumption of the downward trend observed until 2022: as US hyperscalers dramatically accelerate investment in cloud and AI services, creating capabilities European providers cannot match, existing regulatory protections fail to meaningfully reduce lock-in or enable genuine data portability, while aggressive bundled pricing and occasional provider failures erode enterprise confidence in European alternatives. By contrast, the 17% optimistic scenario envisions a more favourable environment where stronger existing regulations ensure genuine interoperability between cloud platforms, reliable data portability safeguards reduce switching friction, and clearer security standards boost customer trust, enabling European providers to convert sovereignty conscious customers such as the public sector and expand into segments currently dominated by hyperscalers.

5.2. Description of the policy options

This section structures the policy options by problems as identified in section 2. The options for problem 1 combine measures of different regulatory intensity and different calibrations of EU versus national delivery. The options for problem 2 are presented along a gradient of intensity of the intervention. Problem 1 and 2 interplay with each other since they concern successive steps of the same value chain, and a supply-demand relationship naturally exists: cloud and AI computing services can only be delivered if the underlying infrastructure exists. Conversely, DC operators only invest based on the expected uptake of their future capacity. The policy options are nevertheless dealt with separately as they correspond to very different realities (physical world vs. dematerialised services), contain policy measures of a different nature and mostly concern different stakeholders. Problem 1 concerns the provision of physical infrastructure (data centres, land availability, permitting, grid connection, connectivity, etc.) mainly involving data centre operators (i.e. colocation providers and, CSPs when they operate their own infrastructure), utilities, local authorities and investors. Conversely, problem 2 concerns the market for cloud and AI computing services, which is shaped by very distinct market and competition dynamics. These two markets are governed by distinct regulatory and economic mechanisms, which call for

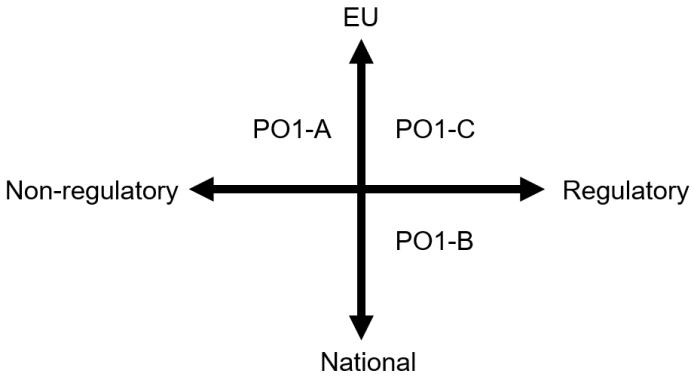
different sets of measures. This approach has allowed to assess the impacts of measures focusing on each of the two problems separately, i.e. infrastructure-related constraints vs market dynamics in the delivery of services, while still recognising their interdependence.

5.2.1. Policy Options to address the limited and geographically concentrated availability of computing capacity in the EU

Table 4. Overview of the first set of policy options, responding to Problem 1

Policy Option PO1-A	Policy Option PO1-B	Policy Option PO1-C
Enhancing the existing collaborative framework	*Legislative and financial intervention enforced nationally*	*Legislative and financial intervention enforced at EU-level*
PM1 - Cloud Alliance expansion PM2 - Data Centre Forum PM3 - Data Centre guidelines	PM4 - National facilitator PM5 - Fast-track areas PM6 - National funding support PM7 - Deployment targets	PM8 - EU R&D funding PM9 - EU deployment funding for strategic projects PM10 - EU-level fast-track

Figure 8. Illustration of policy options to address the limited availability of computing capacity



PO1-A could be combined with both PO1-B and PO1-C. However, PO1-B and PO-C are designed as mutually exclusive. PO1-B packages measures that put Member States in the driving seat, whereas PO1-C places the implementation at the EU-level. See also section 7.7.

Policy Option PO1-A: Enhancing the existing collaborative framework

This policy option strengthens existing collaborative mechanisms between Member States, EU institutions, industry stakeholders and research bodies to support DC expansion. It addresses the identified regulatory and coordination failures through soft measures. Participation and adherence to produced guidelines would remain voluntary.

- **Policy Measure 1 (PM1)** creates a new working group for DC operators in the existing Alliance for Industrial Data, Edge and Cloud, enabling exchange of best practices on deployment, and regular institutionalised dialogue between DC operators, Member State representatives and European CSPs. The working group would be chaired by a representative of the DC industry, with the Commission providing the secretariat.
- **Policy Measure 2 (PM2)** establishes a broader forum for public-private stakeholders (DC operators, TSOs, connectivity providers, equipment manufacturers, and local authorities), enabling coordination and dialogue on DC projects and on the integration of innovative solutions in DCs. It would be convened by the Commission and can build on existing ad hoc DC grid integration roundtables.
- **Policy Measure 3 (PM3)** consists of adopting EU-level guidelines for deploying sustainable DCs. These would go beyond best practices on energy efficiency[clxiv] and would offer guidance on deploying a sustainable DC. They would include recommendations on identifying suitable

land for deployment. Leveraging the forum created under PM2, the guidelines would be co-developed by its participants and subject to periodic review.

This option is a soft way of addressing PD2 (bottlenecks slowing down data centre build-out) While they do not directly change factors like permitting or access to energy, they intend to make them less of a bottleneck by establishing direct links between the actors that are crucial for driving data centre build-out and improving information flows between them (e.g. between data centre operators and TSOs on grid capacity needs). The exchange of best practices among data centre operators will help the industry better navigate the deployment environment in the EU and guidelines will help industry identify, for example, the areas in which data centre deployment may unfold more quickly due to available grid capacity. Beyond specific projects, the interactions between relevant parties would feed into guidelines for data centre deployment – a collection of best practices to be leveraged for faster data centre build-out across the EU. This option would improve the connection between European CSPs (existing Alliance members) and key data centre players (future Alliance members under this option). This would improve opportunities for European CSPs to access data centre capacity or participate directly in the build-out.

The existing Cloud Alliance is a vibrant community of cloud companies which collaborate around projects of common interest and are generally eager to extend membership up/downstream, i.e. to DC operators and their equipment manufacturers. As part of the public consultation, 85% of business respondents (n=52) supported the development of EU guidelines.

Policy Option PO1-B: Legislative and financial intervention enforced nationally

This second policy option consists of legislative and financial intervention implemented at national level, where the EU-level intervention is limited to a coordination role.

- **Policy Measure 4 (PM4)** obliges Member States to designate a national facilitator for all DC projects. Member States would be free to designate as facilitator the entity that suits the task best within their own national structures, for example a service within their central administration or an agency. The facilitator would accompany the applicants from start to finish of the DC project for all authorisations relevant to DC rollout, i.e. planning and building permits, environmental assessments, water and heat use authorisations, and grid connections. Where needed, the facilitator would escalate issues for rapid resolution and interact with the designated facilitator in another Member State if needed for a specific DC.
- **Policy Measure 5 (PM5)** on the basis of a national data centre strategy, obliges Member States to identify suitable areas to fast-track the deployment of DCs. The identification process would follow commonly defined EU-level criteria and ensure that the area displays the necessary characteristics for DC deployment, e.g. connectivity and guaranteed existing or future grid availability. Within these areas, Member States would be required to enact – based on their choice - measures for accelerated DC deployment, beyond administrative acceleration for environmental screenings and communicate clearly on the applicable procedures and criteria. This could include a particular end use for the Data Centre such as being part of a broader digital ecosystem implementing the Apply AI objectives of the Union. The toolbox established in the new Regulation on speeding-up environmental assessments would be leveraged for designated areas, to allow them to benefit from the additional favourable provisions in environmental assessments. In designating the area and designing the related acceleration measures, Member States would receive support from an EU-level coordination hub. Established within the Commission, the hub will offer technical assistance to Member States. The designation of acceleration zones could include an EU-level mechanism to attract smaller users of collocation capacity. Where such status exists in the national context and beyond environmental assessments, DCs would receive favourable status in administrative procedures as projects of highest national significance. In identified suitable sites, Member States would be

bound to the target of reaching a maximum timeline of 18 months for all relevant permits beyond environmental assessments[90]. Some fast-track areas would be reserved to DCs that are of a particular added value to the EU, for examples based on their innovation or sustainability performance (measured in line with the upcoming rating scheme under the EED) or because of the users they will serve. Accordingly, access requirements in terms of sustainability would be defined at EU level but would leave freedom to Member States to add criteria.

- **Policy Measure 6 (PM6)** consists of the possibility of Member States to voluntarily grant public support in line with applicable State aid rules to particularly innovative and sustainable DC projects located in the fast-track areas of PM5 (as with PM5, the sustainability performance would be in line with the EED's rating scheme). Public support could take the form of tax incentives and consider rewarding DCs which contribute positively to grid flexibility and stability.
- **Policy Measure 7 (PM7)** sets an EU-wide DC capacity target which Member States must collectively reach by 2035 and an EU-level monitoring of the progress towards reaching the target. The capacity target would be formulated in MW of DC capacity and would aim to close the compute capacity gap while monitoring of capacity growth in underserved regions, thereby fostering a more geographically balanced distribution of such capacity over time. The monitoring would be integrated into the existing digital decade cycle which would result in an annual report on progress – both at EU and Member State level.

This policy option would help overcome the identified bottlenecks currently slowing down data centre deployment (PD2): The identification of suitable sites for DC deployment is a time-consuming and cumbersome step usually undertaken solely by DC investors who work on the basis of incomplete or inaccessible data (e.g. there's no publicly accessible repository of areas with electricity availability). The national facilitator would help data centre operators navigate permitting requirements and help relevant authorities process requests as efficiently as possible. Rather than altering permitting procedures and changing local requirements, this option addresses regulatory complexity by making it more navigable for data centre operators and ensuring fastest possible treatment within fast-track areas. The designation of fast-track areas would help data centre operators identify suitable land. These measures would also aim to improve transparency and coordination around zoning and grid access to facilitate more contestable access to key inputs. Through the option for national funding, this option allows the de-risking of investments in strategic data centre projects, helping overcome access-to-capital issues. This can prove particularly beneficial for European providers to gain access to data centre capacity or participate in the build-out themselves, which can boost the scale and scope of services provided by Europeans (PD1).

Respondent views on Policy Option PO1-B. Feedback from DC operators from the public consultation (n=30 respondents) on measures under this policy option:

Measure	Overall support
One-stop-shop service to simplify infrastructure permitting procedures	**83%**
Expedited approval mechanisms and clear conditions for strategic or critical projects	**97%**
Public-private partnerships for large-scale data centres	**63%**
Tax incentives for using sustainable technologies	**73%**

There has been noticeable support in the Call for Evidence (CfE) for measures within PO1-B. Most companies and business associations favour simplification of permitting requirements,

[90] Annex 4, section 8 presents the relevant permitting steps and their relative duration in 12 Member States. The necessary improvements to grid availability will be driven by the Grids package (see section 5.3).

introducing a national facilitator for DC projects, and fast-track mechanisms. Some respondents suggested faster grid connection and the creation of special DC deployment areas established at national level.

Policy Option PO1-C: Legislative and financial intervention enforced at EU-level

This third policy option introduces binding acceleration measures enacted at EU-level and supported with EU funding.

- **Policy Measure 8 (PM8)** identifies the key EU-level R&D funding challenges to the development of energy- and resource-efficient and secure DC technologies, including advanced cooling, renewable energy and storage integration, and AI-based optimisation tools[91]. While a fictitious amount is set for modelling purposes, the initiative would not mention a specific amount, thus not pre-empting the MFF discussions.
- **Policy Measure 9 (PM9)** creates the possibility, without prejudice to the outcome of the negotiations on the next MFF proposal, for strategic DC deployment projects to be supported by Union programmes, funds and financial instruments, in accordance with the objectives set out in the regulations establishing those funds and programmes, in particular those implementing the EU's vision for an AI continent / Apply AI. The Cloud and AI Development Act would specify binding EU-level criteria in accordance with which strategic projects would be identified by the EC. As with PM8, a fictitious amount is used for modelling, while the initiative would only be declarative.
- **Policy Measure 10 (PM10)** empowers the Commission to designate suitable areas for accelerated DC deployment following EU-level criteria and in consultation with Member States experts within an EU DC Acceleration Board. This Board would be created as a dedicated committee (comitology). Permit granting for DC projects would follow EU-wide rules and require approval from the Board. For these areas, Member States would be required to enact a set of acceleration measures prescribed at EU level. The toolbox established in the new Regulation on speeding-up environmental assessments would be leveraged for DC projects deployed in these areas, to benefit from the additional favourable provisions in environmental assessments.

By centralising the designation of areas and processes for accelerated deployment under an EU expert body, this policy option would tackle the bottlenecks to DC expansion (PD2). Direct funding for the development of sustainable DC technologies and support to DC integrating such technologies would increase sustainable capacity. In terms of substance, this option has roughly the same thrust as PO1-B, but with EU-level decision-making and the use of EU funds for R&D and the deployment of strategic data centres. While open to all data centre operators, this option will also benefit European cloud and AI service providers where they themselves seek to build data centres or rent newly created co-location capacity. The measures thus also contribute to addressing the lack of scale and scope of EU cloud service providers (PD1) whose ability to scale, as described in section 2.2.1., is – among other factors – restricted by their limited infrastructure presence and the high costs of expanding it.

In response to the CfE, several companies, business associations and a Member State expressed support for R&D funding at national and EU level. Respondents generally showed strong support for measures that would advance the energy efficiency performance of data centres. In the questionnaire (n=243), 70% of respondents supported funding for R&D of energy-efficient technologies.

[91] Such as AI solutions for optimising the operation of DCs.

5.2.2. *Policy Options to address the dependence on cloud and AI computing services supplied by non-European providers*

Table 5. Overview of the second set of policy options responding to problem 2

Policy Option PO2-A	Policy Option PO2-B	Policy Option PO2-C
Supporting measures to increase transparency and visibility of sovereign cloud and AI computing services	*Voluntary framework for advancing sovereign cloud and AI computing services*	*EU-coordinated procurement and support framework for sovereign cloud and AI computing services*
PM11 – Creating EU-level harmonised criteria for sovereign cloud and AI computing services PM12 – EU guidelines on the requirements to be fulfilled by sovereign cloud and AI computing services PM13 – Annual conference on EU Digital Sovereignty PM14 – Interoperability flanking measures	PM15 – Voluntary sovereign risk assessments for the use of cloud & AI computing services in the public sector PM16 – Voluntary award criteria PM17 – Public sector cloud federation and EU broker PM18 – Vendor-neutral cloud and AI training programme	PM19 - Mandatory award criteria PM20 – Open Source use in the public sector PM21 – Mandatory sovereign risk assessments for the use of cloud and AI computing services PM22 – Joint EU-level procurement of cloud and AI PM23 – SME cloud and AI support scheme PM24 – Cloud and AI toolbox

PO2-A packages measures which require EU action but without binding effects. PO2-A can be implemented together with both PO2-B and PO2-C. PO2-B represents an increasing level of EU involvement. PO2-C strengthens this further and covers binding measures. PO2-B and PO2-C are not per se mutually exclusive but some measures in PO2-C represent a different gradient of intervention from similar measures in PO2-B. Figure 9 illustrates how individual measures from each PO build on each other, making them mutually exclusive. The relationship between the options below and the identified problem drivers is discussed jointly at the end of this section.

Policy Option PO2-A: Supporting measures to increase transparency and visibility of sovereign cloud and AI computing services

This policy option aims at establishing a common understanding of the notion of sovereignty for cloud and AI computing services and increasing their visibility on the market. It is complemented by a flanking measure to ensure the participation of European providers in the development of interoperability standards.

- **Policy Measure 11 (PM11)** establishes a harmonised Union-level framework for sovereign cloud and AI computing services. AI systems (which are products and not services) are not concerned by the measure, as they are already subject to the AI Act. Acknowledging that different use cases require varying degrees of 'sovereignty', the framework provides for four levels of sovereignty assurance. Services not meeting any of the conditions would not be classified with any sovereignty level but would obviously remain available in the market.

  To be considered '***sovereign level 1'***, a service must meet the following cumulative criteria:
  (i) the service provider must be **established** in the Union; and
  (ii) the service must be fully operated from computing infrastructure, personnel and assets **located** in the Union (meaning the EEA); and
  (iii) customer data, including metadata and telemetry data, is in the EU unless the customer explicitly requires otherwise; and
  (iv) the service provider demonstrates that it complies with state-of-the-art cybersecurity standards; and
  (v) if technical and operational support is outsourced to third-party providers outside of the Union, necessary measure are put in place to ensure that would not compromise the provider's operational autonomy; and

(vi) there is full transparencey around the use of subcontractors, for which the cloud service provider assesses that they meet Union legal obligations; and
(vii) where the cloud service provider is subject to the control of a third country or a third country entity, it must be able to prove that the laws and government practices in that country do not require the provider to tell that country's authorities about software vulnerabilities before those vulnerabilities have been publicly discovered

These requirements **would allow** service providers with a parent company headquartered outside of the Union to be considered as 'sovereign level 1'.

To be considered '***sovereign level 2***', a service must meet the following cumulative criteria:
(i) the service provider and subcontractors must be **established** in the Union; and
(ii) the service must be fully operated from computing infrastructure, personnel and assets **located** in the Union; and
(iii) provide available personnel complying with additional personnel screening and Union citizenship requirements, if the customer determines that imposing these additional requirements is necessary; and
(iv) the service provider must be **controlled** by a legal entity in the Union. Alternatively, if the service **is controlled by a third-country legal entity**, it must demonstrate that it has in place the necessary technical, legal and organisational measures necessary to prevent third-country governmental access and transfer of data stored in the Union, to prevent or refuse any request from a third-country government, ensure that the control of the third-country or third-country entity is not exercised in a manner that restricts the provider's ability to deliver the service, and to prevent the service disruption and/or degradation of the service by a third-country government[92]; and
(v) the data generated by using the audited service shall not be re-used for the training or fine-tuning of an AI system **operated by an entity outside the EEA and in any case are not transferred outside the Union**; and
(vi) the customer data, including metadata and telemetry data, remain in the Union unless the customer explicitly requests otherwise; and
(vii) the service must demonstrate a high level of cybersecurity by being certified at least at level '**substantial**' under the European Cybersecurity Certification Scheme for Cloud Services (EUCS) [93]; and
(viii) the service provider must demonstrate a **high degree of control** over the software components that underpins the service. This notably implies that there exists a list of identified dependencies related to the provision of the service, and where the software components are provided by a third-country entity, **the relevant code** of the **security relevant components** of the service stack can be audited, and there exists a migration plan in the event a vendor fails or a third-country imposes restrictions; and
(ix) if the subcontractors are from a third country or a third country entity, appropriate measures in place to demonstrate the absence of control; and

[92] In the absence of a harmonised framework, non-EU service providers attempting to prevent third-country governmental access and transfer of data stored in the Union and to prevent or refuse any request from a third-country government are using a diverse technical, legal and organisational measures. This include technical architecture with segregated physical infrastructure, ensuring that the encryption keys are not accessible to the provider or are held exclusively by the customer, adding specific clauses in their EU employees' contract that forbid them from taking instructions from outside of the EU, setting up independent boards to review extra-territorial data access requests, etc.
[93] As part of the '*One Europe, one market'* roadmap agreed by the Parliament, the Council and the Commission, the co-legislator have agreed to finalise negotiation for this initiative ed by Q4 2027. Adding one year for the measures to take effect, this implies CADA entering into force in early 2029. EUCS technical work is finalized and has been adopted by CEN-CENELEC Technical Specifications. The candidate scheme has therefore reached an advanced stage of development, which now needs to be transformed into an Implementing Act adopted under the Cybersecurity Act, a process much shorter than CADA's interinstitutional negotiations.

(x) operational and technical support, including outsourcing, are initiated and performed exclusively within the Union; and
(xi) where the cloud service provider is subject to the control of a third country or a third country entity, it must be able to prove that the laws and government practices in that country do not require the provider to tell that country's authorities about software vulnerabilities before those vulnerabilities have been publicly discovered

These requirements **would allow** service providers controlled by a third-country or third-country entity to be considered as 'sovereign level 2', but on the basis of some organisational efforts. Service providers owned and controlled by a legal entity in the Union would face less difficulties in complying with these criteria.

To be considered '***sovereign level 3***', a service must meet the following cumulative criteria:
(i) the service provider and subcontractors must be **established** in the Union; and
(ii) the service must be fully operated from computing infrastructure and assets **located** in the Union; and
(iii) members of the board, executive team and personnel operating the service are Union nationals, located in the Union, **and are security cleared where appropriate**; and
(iv) the service provider must be **owned and controlled** by a Union legal entity and the subcontractors are not subject to the control of a third country or a third-country entity. A cloud computing service subject to the control of a third country or a legal entity established in a third-country can still be audited against the audit criteria where the third country has implemented specific safeguards that ensure that there is no risk of unauthorised access to Union data or possible disruption of service quality or continuity; and
(v) the data generated by using the audited service shall not be re-used for the **training or fine-tuning of an AI system** operated by an entity outside the Union and **in any case are not transferred outside of the Union**, and
(vi) the customer data, including metadata and telemetry data, remain in the Union unless the customer explicitly requests otherwise; and
(vii) the service must demonstrate a high level of cybersecurity by being certified at least at level 'substantial' under the European Cybersecurity Certification Scheme for Cloud Services (EUCS); and
(viii) the service provider must demonstrate **a high degree of control** over the software components that underpin the service (software stack). This notably implies that there exists a list of identified dependencies related to the provision of the service, and where the software components are provided by a third-country entity, the **relevant code** of the **security relevant components** of the service stack can be audited, and there exists a migration plan in the event a vendor fails or a third-country imposes restrictions; and
(ix) operational and technical support, including outsourcing, are initiated and performed exclusively within the Union and by Union citizens, and by third parties that are not subject to the control of a third country or third country entity; and
(x) where the cloud service provider is subject to the control of a third country or a third country entity, it must be able to prove that the laws and government practices in that country do not require the provider to tell that country's authorities about software vulnerabilities before those vulnerabilities have been publicly discovered.

These requirements **would <u>not</u> allow** service providers whose parent company is headquartered outside of the Union to be considered as 'sovereign level 3'.

To be considered '***<u>sovereign level 4'</u>***, a service must meet the following cumulative criteria:

(i) the service provider, and subcontractors must be **established** in the Union; and
(ii) the service must be fully operated from computing infrastructure and assets **located** in the Union; and
(iii) members of the board, executive team and personnel operating the service are Union nationals, located in the Union, **and are security cleared where appropriate**; and
(iv) the service provider must be **owned and controlled** by a Union legal entity and the subcontractors involved in the provision of the service are located in the Union, owned and controlled by a Union legal entity; and
(v) the data generated by using the audited service shall not be re-used for the training or fine-tuning of an AI system **operated by a third-country legal entity and in any case are not transferred outside of the Union**; and
(vi) the customer data, including metadata and telemetry data, remain exclusively in the Union; and
(vii) the service must demonstrate a high level of cybersecurity by being certified at least at level 'high' under the European Cybersecurity Certification Scheme for Cloud Services (EUCS); and
(viii) the service provider must demonstrate **effective control** over the software components that underpin the service (software stack) by demonstrating that a third country or a third country entity does not have excessive control over the software lifecycle. This notably implies that the **relevant code** of the service stack can be audited and that effective control of the code exists by a Union legal entity; and
(ix) operational and technical support, including outsourcing, are initiated and performed exclusively within the Union and by Union citizens, and by third parties that are not subject to the control of a third country or third country entity; and
(x) where the cloud service provider is subject to the control of a third country or a third country entity, it must be able to prove that the laws and government practices in that country do not require the provider to tell that country's authorities about software vulnerabilities before those vulnerabilities have been publicly discovered

These requirements **would <u>not</u> allow** providers headquartered outside of the Union to be considered as 'sovereign level 4'.

These criteria above deal with sovereignty. Cybersecurity and sovereignty are closely related and are complementary. However, they do not focus on the same aspects nor pursue identical objectives. The Commission, through its own tendering for EUR 180 m of sovereign cloud services, was able to test the feasibility of such definitions established in different levels and could verify that it can be implemented.

	Control	EU infra-structure	Personnel	AI inference data	Supply chain	Sub-contractors	Vulnerability disclosure restrictions	Cybersecurity	Type of assessment
Level 4	EU established, owned and controlled	Fully located in the Union	Located in the EU and EU citizens. Security cleared (**)	Not transferred outside of the EU and not reused by a third-country entity	Effective control (over the software)	Established in the Union, owned, and controlled	Not needed	High	National authorities based on a 3rd party-audit
Level 3	EU established, owned and controlled (*)	Fully located in the Union	Located in the EU and EU citizens. Security cleared (**)	Not transferred outside of the EU and not reused by a third-country entity	High degree of control (auditable software)	Established in the Union. If owned by a 3rd country, absence of interference (*)	No hidden disclosures	Substantial	National authorities based on a 3rd party-audit
Level 2	EU established & absence of 3rd country interference	Fully located in the Union	Located in the EU. EU citizens if required by the customer	Not transferred outside of the EU and not reused by a third-country entity	High degree of control (auditable software)	Established in the Union. If owned by a 3rd country, absence of interference	No hidden disclosures	Substantial	National authorities based on a 3rd party-audit
Level 1	EU established	Fully located in the Union	Located in the EU	No requirement	No requirement	Full transparency	No hidden disclosures	State-of-the-art cybersecurity standards	Self-assessment

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

Types of providers whose services could currently reach sovereignty Levels 1-4

Level 1: US hyperscalers generally all have offerings that would allow them to qualify under Level 1. They offer dedicated EU-based cloud services with strong cybersecurity credentials which rely exclusively on (data) 'regions' located in the EU, including for redundancy.

Level 2: Several US hyperscalers have partnered with EU companies to provide additional sovereignty assurances – these partnerships are often called "sovereign joint ventures". While the implementation models differ, such partnerships generally rely on majority EU ownership, operation by EU personnel, data centre region limited to a particular Member State, cloud software stack provided by a hyperscaler, with security layer controlled by the EU partner, auditable core software, with some reaching certification under the SecNumCloud scheme. Non-European companies, outside of joint ventures, could also qualify provided they demonstrate the absence of 3rd country interference.

Level 3: EU providers would easily satisfy the control criteria. They would have to pass the necessary cybersecurity controls to achieve the future EUCS certification at assurance level Substantial or High. The other difficulty would be to demonstrate a 'very high' control over their software supply chain, something demonstrated in the recently awarded contract by the Commission for sovereign cloud services.

Level 4: This level differs from level 3 in stricter cybersecurity certification and full control over the software supply chain, something that some emerging EU offerings propose, at least for some type of cloud services.

- **Policy Measure 12 (PM12)** foresees the adoption of guidelines on the harmonised EU-level criteria for sovereign cloud and AI computing services defined under PM11 to help implementation. These guidelines would be adopted by the Commission, addressing expectations towards providers and users about what constitutes a sovereign service.
- **Policy Measure 13 (PM13)** addresses information asymmetries through awareness raising for the sovereignty common understanding and other measures. In particular, an annual week-long EU-organised conference on digital sovereignty, bringing together academic institutions, researchers, and overall public and private stakeholders to foster collaboration in cloud and AI innovation and the development of sovereign cloud and AI computing services. The EU-organised awareness raising efforts would centralise the currently scattered efforts of private sector entities to enhance the visibility of sovereign services and create a forum for providers to connect with prospective buyers from the private and public sector.
- **Policy Measure 14 (PM14)** sets up measures ensuring the effectiveness of the interoperability provisions of the Data Act: A Commission-led coordination group with Member States and industry to drive progress on the development of interoperability standards. This would serve as a preparatory step to the standardisation requests which the Commission can issue under the Data Act. In addition, the measure creates a hook for possible financial support, in the context of the next MFF (but without prejudging the outcome of such negotiations), for EU industry participation in EU standardisation organisations to ensure that the perspective of smaller European service providers is represented when these organisations work on a standardisation request issued under the Data Act.

In response to the CfE, many European companies favoured a harmonised sovereignty criteria at EU level. Public authorities showed strong support for the development of operational sovereignty criteria. Some companies and business associations, especially located outside the EU, stressed that such criteria should not exclude providers merely based on headquarters location.

Policy Option PO2-B: Voluntary framework for advancing sovereign cloud and AI computing services

This option contains measures which go beyond defining and making more visible sovereign services. They create a legislative framework for identifying such services, leaving its use voluntary. The measures also target the broader uptake of a more diverse set cloud and AI computing services in the public and private sector.

- **Policy Measure 15 (PM15)** would **recommend** Member States to carry at least one sovereignty risk assessment and repeat it at least every four years but more frequent if deemed necessary. The purpose of the sovereignty risk assessment is to identify which public sector use cases within a Member State require the use of which sovereignty level as described under PM11. The sovereignty risk assessment would assess, *inter alia*, the risks induced by the access to such data by a third-country authority or third-country legal entity; or the risk of possible service disruption due to dependence on a single or limited number of third-country services providers.

  On the basis of dedicated discussions conducted with 3 different public authorities representing about 200 NIS2-Annex 1 contracting authorities, operating at regional, national and European level (out of an estimate of 6 400 NIS2 entities across the EU), this assessment assumes that the matching of sovereignty levels to public sector demand follows the following pattern: 70% of use cases would require a sovereignty level 1; 20% for level 2; 9% for level 3; and 1% for level 4. Even though the scheme is novel and does not correspond to existing frameworks, this assessment fits with broad orders of magnitude that can be inferred from existing analyses

conducted in several Member States that have introduced risk assessments for their public sector clouds, such as France, Poland[94] or Italy[95].

This approximation is anchored in the idea that a layered and progressively more demanding criteria is designed to tackle a progressively smaller amount of use cases. For instance, a water supply public company might have separate IT systems to deal with non-critical use cases, but fewer to manage critical systems.

Table 6. Illustrative distribution of criticality of IT systems within a fictitious public sector water company

Non-critical use cases (candidate for level 1)	Critical use case (candidate for levels 2-4)

• **Procurement**
• **Stock management**
• **Inventory**
• **Helpdesk**
• **Billing system**
• **Accounting system**
• **CRM**
• **Workforce management**:
  ○ **Payroll**
  ○ **Timesheets**
  ○ **Training**
  ○ **Holidays**
  ○ **Recruitment**
  ○ …
• **…**
	• Water monitoring system
	• Incident response system
	• Early warning system

In concrete terms, France's SecNumCloud, the closest scheme to this sovereignty framework, was developed acknowledging that there is demand for even higher levels of sovereignty for the most sensitive use cases, estimated at 10% of all public sector use cases (which here correspond to sovereignty level 3 and level 4). Conversely, out of the remaining use cases (90% of all public sector use cases), the scheme was designed to address approximately only ⅕ to ¼ of them (that is approximately 18% to 22.5% of all public sector use cases). While the individual criteria under SecNumCloud are not the same, the compound effect of level 2 criteria under CADA allows the same type of providers (having implemented the same type of mitigating measures) to qualify for this level. The proportion of 20% (rounded up mean value of 18% and 22.5%) was therefore retained as a first approximation for the proportion of all public sector use cases where conformity with level 2 would be required.

Critical use cases, defined as the use cases whose disruption would affect operational autonomy or public order, correspond to use cases covered by level 2, 3 and 4, so 30%. The risk assessment would have to consider the reality of the supply market to avoid unrealistic outcomes, such as mandating the use of services that don't exist (yet) in the market. The measure targets critical use cases, not individual public authorities, but it is likely that Member States would focus on the public sector entities of high criticality (as defined in NIS2 annex 1), which amount to 6 400 throughout the EU, an amount retained in this assessment where such data point is needed. This figure results from the amount of NIS 2 entities in Europe (160

[94] See Cloud in Government Services
[95] See Strategia Cloud Italia

000[96]), from which 20% are essential entities under Annex I[97], from which 20% are assumed to be public entities: 160 000 * 20% * 20% = 6 400 NIS2 Annex 1 public sector entities.

To facilitate appropriate and coherent sovereignty risk assessments, the European Commission would develop guidelines for Member States to conduct such assessments and provide a sample risk assessment methodology (note that these guidelines concern the conduct of risk assessments and differ from PM12, which consist in explaining the different levels of sovereignty). For Member States to have up-to-date information about the market conditions of cloud and AI sovereign solutions, the Commission would also produce market monitoring reports that will point Member States to possible gaps in the coverage of some services.

The Member State would be **recommended** to reflect the outcome of the risk assessment in applicable public tenders, unless duly justified.

While PM11 only puts forward the definition of sovereignty levels, PM15 goes further by putting forward a framework through which the respective levels of sovereignty can be assessed. Verifying compliance against sovereignty level 1 would be based on self-assessments conducted by the service provider. Cloud computing service providers qualifying as SMEs would not be required to undergo the validation by the national competent authority.Verifying compliance of service against sovereignty level 2-3-4 would be done through third party's auditors and verified by national competent authorities designated by Member States.. The competent authorities will then verify the audit report, opinion and evidence and will provide the decision that would allow the service provider to participate in procurement procedures across the Union that are limited to the respective assurance level. Other Member States shall be notified of the draft decision, to which they can object within 60 days. If continued objections occur, the Commission will adopt a binding decision.

The competent authorities should also register the audit approval in a Union repository, maintained by the Commission. The repository of sovereign cloud and AI computing services will be a public list of audited sovereign cloud and AI computing services that verifiably comply with the sovereignty requirements. The benefits are for providers and users alike: providers will enhance their visibility and users their market research.

To cater for market evolutions, the sovereignty criteria of all levels and evaluation methodology would be modifiable by comitology. This evaluation methodology would help third party auditors in their assessment of the service and ensure full harmonisation in the way different auditors conduct their assessment and for Member States to ensure that the procedures have been followed.

The outcome of the audit would be valid across the Union, with a recourse possibility for providers and Member States. Other Member States and the European Commission shall also have the possibility to request clarifications about certifications granted by other MS. The assessment would be renewable following the same evaluation methodology.

This measure is primarily designed to contribute to the protection of public order by enhancing the resilience in the public sector, which is SO4. Nevertheless, European providers would face less costs and efforts to meet sovereignty conditions. When it comes to meeting the criteria to

[96] See SWD published as part of the proposal for the Digital Omnibus
[97] This is an extrapolation to the EU of France's NIS2 available data

demonstrate sovereignty level 1 and 2, EU providers can more readily substantiate that they are not affected by third-country policies affecting data access or limiting service continuity. As well, level 3 and level 4 sovereignty can only be served by service providers owned and controlled by EU entities. This implies that PM15 will also contribute to decreasing the overall reliance on non-European cloud and AI computing services, which is SO3.

- **Policy Measure 16 (PM16)**, with a view to support the EU added value provided by public procurement of cloud and AI computing services, this measure establishes a set of **voluntary** non-price award criteria for the public procurement of cloud and AI computing services. The criteria should be of ancillary and non-decisive value in view of the overall tender and are to be included, voluntarily, by contracting authorities in the procurement of cloud and AI computing services that are not off the shelf, standardised or commercially available services. These criteria will earn additional points to tenderers that demonstrate:
  (i) That the tenderer contributes to reinforcing the digital technology supply chain in the Union, including the use of software or hardware designed or manufactured in the Union
  (ii) That the tenderer has integrated Union technologies, including the uptake of research and development results stemming from EU-funded research and development programs;
  (iii) That the innovation required to deliver the service being procured is conducted in the Union or in a third country that contributes to the development of a European cloud and AI ecosystem;
  (iv) That the service is delivered, to the greatest extent feasible with regard to market availability or technical requirements, through critical [computing, storage and networking] hardware components designed in the Union or manufactured in the Union, or both, or, where this is not feasible, through hardware components from a country or countries that contribute to strengthening security of supply and developing a European cloud and AI ecosystem;
- **Policy Measure 17 (PM17)** establishes a voluntary public sector cloud federation of EU institutions, bodies and agencies, Member States and other public sector bodies. Members of the federation would be allowed to share the DC services, cloud and AI computing services which they own and control. This measure requires the Commission to create a platform providing a brokering service. The Commission and the Member States would adopt the required non-functional service level agreements (e.g. uptime) and the harmonised technical specifications.
- **Policy Measure 18 (PM18)** creates a vendor-neutral cloud and AI training programme to upskill workers in the single market, particularly addressing the interconnection between these services and their underlying technologies. This implies developing curricula and certification mechanism and funding the institutions delivering the training. The initiative would be declarative, without financial commitments.

Among public authorities that replied to the public consultations, 77% support mechanisms to allow the federation of cloud and AI computing services between public administrations within and across Member States. In terms of EU-level action, 53% of total respondents support the inclusion of a criterion ensuring sovereignty, autonomy, resilience and availability to help public administrations in their procurement process. This measure was supported by 77% of public authorities. 85% were in favour of guidelines with standard criteria for procuring cloud and AI computing services. Several respondents expressed support for skills training programs in both the public and private sectors.

Policy Option PO2-C: EU-coordinated procurement and support framework for sovereign cloud and AI computing services

This option leverages PO2-B (and by extension one element from PO2-A, see Figure 9) to foster the uptake of cloud and AI computing services in the public and private sector, with a higher level of EU intervention and mandatory requirements for the public sector.

- **Policy Measure 19 (PM19): First,** with a view to reducing critical dependencies, this measure makes the use of the non-price award criteria under PM16 mandatory. When procuring cloud and AI computing services for which the EU has been assessed as dependent, contracting authorities would be obliged to apply the award criteria established under PM16.

  Second, Member States would have to draft an action plan to explain how they intend to use public procurement, notably through pre-commercial procurement and procurement of innovation instruments, to increase the uptake of highly innovative cloud and AI computing services from small-cap companies, notably start-ups and scale-ups. As a follow-up, the uptake of such services, would be monitored through a centralised, Commission-led monitoring exercise. This would avoid the need for separate reporting obligations and create synergies with other measures within this Policy Option that are aimed at assessing the market presence of EU providers (cf. PM21). PM19 will contribute to decreasing the overall reliance on non-European cloud and AI computing services, which is SO3.

- **Policy Measure 20 (PM20)** aims to encourage the share and, reuse of open source assets by the public sector. Under this measure, public authorities are encouraged to promote the use of open standards and available open source solutions where these demonstrate comparative merit to proprietary solutions and reuse digital assets, including code, configurations, and documentation, developed by other public administrations rather than commissioning similar solutions from scratch, thereby eliminating duplication of efforts and redundant expenditure on functionally similar solutions; and to share software into a common repository, ensuring that investments made by public administrations in the EU contributes to a pool of collectively maintained sovereign solutions.

  Therefore, **first**, this policy measure requires Member States to take the necessary measures to encourage the use of open standards and open source software by public sector organisations taking into consideration aspects such as functionalities, total cost, user-centricity, cybersecurity or other relevant justified objective criteria.

  Second, public organisations will have to consider making the software for which they hold rights publicly available on an open source repository connected to the EU OSS catalogue maintained by the Commission. The released software should put in place the appropriate safeguards to protect security or intellectual property rights. To ensure the quality and security of publicly released code, open source repositories will have clear governance and operational mechanisms, such as quality assurance (e.g. DevOps) and the continuous assessment of the cybersecurity posture of the components (e.g. static and dynamic security testing) complemented by a Software Bill of Materials. The release of software as open source shall not be made in the case in which the cost of doing it would be disproportionate, there is a risk to the security of information systems of the Union or there is public order restriction.

  Third, this measure includes the creation and maintenance of Open Source Programme Offices (OSPOs) within the public sector to support the implementation and management of open source software. To facilitate the cooperation among these OSPOs, the Commission will establish a Network of OSPOs.

- **Policy Measure 21 (PM21)** consists of two elements. **First**, it turns what is only a Recommendation under policy measure 15 into **a binding requirement** for Member States.

Member States **shall carry** at least one sovereignty risk assessment and repeat it at least every four years but more frequent if deemed necessary. The purpose of the sovereignty risk assessment is to identify which public sector use cases within a Member State require the use of which sovereignty level as described under PM11. The sovereignty risk assessment would assess, *inter alia*, the risks induced by the access to such data by a third-country authority or third-country legal entity; or the risk of possible service disruption due to dependence on a single or limited number of third-country services providers. On the basis of dedicated discussions conducted with 3 different public authorities representing about 200 contracting authorities, this assessment is based on the finding that the matching of sovereignty levels to public sector demand follows the following pattern: 70% of use cases would require a sovereignty level 1; 20% for level 2; 9% for level 3; and 1% for level 4. Even though the scheme is novel and does not correspond to existing frameworks, this assessment fits with broad orders of magnitude that can be inferred from existing analyses conducted in several Member States that have introduced risk assessments for their public sector clouds, such as France, Poland[98] or Italy[99]. This approximation is anchored in the idea that a layered and progressively more demanding criteria is designed to tackle a progressively smaller amount of use cases. For instance, a water supply public company might have separate IT systems to deal with non-critical use cases (e.g. procurement, stock management, inventory, helpdesk, billing system, workforce management, fleet management, etc), but fewer to manage critical systems (e.g. water monitoring system). For instance, France's SecNumCloud, the closest scheme to this sovereignty framework was developed acknowledging that there's demand for even higher levels of sovereignty, estimated at 10% (which here correspond to level 3 and level 4), and that for the remaining 90%, SecNumCloud was designed to cover 1/5 to 1/4 of the use cases, so somewhere in between 90% * 1/5 = 18% and 90% * 1/4 = 22.5%. While the criteria for SecNumCloud and level 2 differ, this figure is nevertheless retained as a first approximation.

Critical use cases, defined as the use cases whose disruption would affect operational autonomy or public order, correspond to use cases covered by level 2, 3 and 4. The risk assessment would have to consider the reality of the supply market to avoid unrealistic outcomes, such as mandating the use of services that don't exist (yet) in the market.

The measure targets critical use cases, not individual public authorities, but it is likely that Member States would focus on the public sector entities of high criticality (as defined in NIS2 annex 1), which amount to 6 400 throughout the EU, an amount retained in this assessment where such data point is needed. This figure results from the amount of NIS 2 entities in Europe (160 000[100]), from which 20% are essential entities under Annex I[101], from which 20% are assumed to be public entities: 160 000 * 20% * 20% = 6 400 NIS2 Annex 1 public sector entities.

To facilitate appropriate and coherent sovereignty risk assessments, the European Commission would develop guidelines for Member States to conduct such assessments and provide a sample risk assessment methodology (note that these guidelines concern the conduct of risk assessments and differ from PM12, which consist in explaining the different levels of sovereignty). For Member States to have up-to-date information about the market conditions of cloud and AI sovereign solutions, the Commission would also produce market monitoring reports that will point Member States to possible gaps in the coverage of some services.

[98] See Cloud in Government Services
[99] See Strategia Cloud Italia
[100] See SWD published as part of the proposal for the Digital Omnibus
[101] This is an extrapolation to the EU of France's NIS2 available data

The Member States **would have to** determine which public authorities are required to procure specific levels of sovereignty and make this mandatory at national level, ensuring that procurement aligns with the risk assessment, unless duly justified.

While PM11 only puts forward the definition of sovereignty levels, PM15 goes further by putting forward a framework through which the respective levels of sovereignty can be assessed. Cloud computing service providers qualifying as SMEs would not be required to undergo the validation by the national competent authority. Verifying compliance against sovereignty level 1 would be based on self-assessments conducted by the service provider itself, while assessing the compliance of the service against sovereignty levels 2-3-4 would be performed through independent third party's auditors and verified by national competent authorities designated by the Member States. The competent authorities will then verify the evidence provided by the service providers, the audit report and opinion and will provide a decision: acceptance, rejection or request for further information. If positive, the competent authority of the establishment of the service provider shall notify other MS for objections, which the evaluating competent authority will have to take into consideration for the final decision. This decision will allow the service provider to participate in procurement procedures across the Union. In the case of continued objections, the Commission will assess it and adopt a binding decision to settle the dispute. If the evaluating competent authority determines that there is not enough information to take a decision, it shall request the provider for additional information. Finally, in the case of a rejection, the cloud service provider will have the possibility to recourse, which the evaluating competent authority will have to take into account for the final decision.

Competent authorities should also register the audit approval in a Union repository, maintained by the Commission, as well as on the Digital Wallet of the service provider. The repository of sovereign cloud and AI computing services will be a public list of audited sovereign cloud and AI computing services that verifiably comply with the sovereignty requirements. The benefits are for providers and users alike: providers will enhance their visibility and users their market research.

To cater for market evolutions, the sovereignty criteria of all levels and evaluation methodology would be modifiable by comitology. This evaluation methodology would help third party auditors in their assessment of the service and ensure full harmonisation in the way different auditors conduct their assessment and for Member States to ensure that the procedures have been followed.

This measure is primarily designed to contribute to the protection of public order by enhancing the resilience in the public sector, which is SO4. Nevertheless, European providers would face less costs and efforts to meet sovereignty conditions. When it comes to meeting the criteria to demonstrate sovereignty level 1 and 2, EU providers can more readily substantiate that they are not affected by third-country policies affecting data access or limiting service continuity. As well, level 3 and level 4 sovereignty can only be served by service providers owned and controlled by EU entities. This implies that PM21 will also contribute to decreasing the overall reliance on non-European cloud and AI computing services, which is SO3.

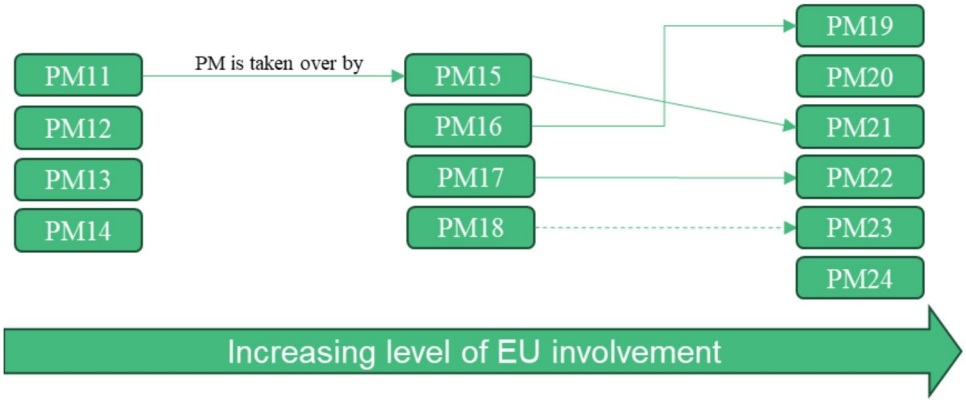
Second, private sector essential entities listed under Annex I of NIS 2 are encouraged to integrate into the cybersecurity risk assessment they already conduct, the assessment of the

risks stemming from their use of cloud and AI computing services. This includes an analysis of the laws applicable to the computing service and the extraterritorial reach of such laws; the risks associated to the possible unauthorised third country government access to and transfer of data; the risks associated to service continuity and quality; the operational dependency and possible loss of autonomy.

- **Policy Measure 22 (PM22)** establishes a voluntary framework for EU-level public procurement of cloud and AI computing services for EU institutions, bodies and agencies, and Member States public sector organisations. The intention of the joint procurement framework is to enable participants to procure with a common voice. The joint procurement framework would complement Member States' existing procurement practices. This measure is about creating a framework enabling joint procurement, but the participating contracting authorities are left with the power to decide the details of what they ultimately want to procure. This measure builds on the common platform under PM17. It will allow aggregation of demand for innovative solutions, allowing the EU to do what the US has done with a lot of success in the past, i.e. award large contracts which support early innovation and uptake (see PD1) and mitigate the lack of stable contracts holding European providers back from scaling up (see PD3).
- **Policy Measure 23 (PM23)** creates a support scheme for SMEs to support through consultancy the adoption of cloud and AI computing services by SMEs, including European CSPs. While technically independent, this measure presents synergies with PM18. As with other measures that imply funding, this does not pre-empt the next MFF.
- **Policy Measure 24 (PM24)** would imply that the Commission sets up an online toolbox for the private sector service providers to easily identify software tools, in particular open source ones, with the specific aim to help them in complementing their service offering. This toolbox would create visibility for lesser known tools and serve as a final repository for the outcome of projects funded by European programmes.

Overall, all the categories of respondents showed strong support for measures that would promote open source, including to achieve sovereignty. Most EU citizens, public authorities and academic institutions would favour an obligation to release the code developed with public money in open source repositories, as well as a common EU open source licensing schema. Public authorities showed strong support for a marketplace for cloud and AI computing services. In terms of EU-level action to prevent unlawful access to data, several public authorities favoured common criteria to help them during the procurement process to identify highly critical use cases. Several companies also supported this. Over 60 position papers received through the CfE stressed the importance of public procurement, including joint procurement and the strategic role the public sector could play as an anchor client.

Figure 9. Illustrations of Policy Options to address the dependence on cloud and AI computing services supplied by non-European providers



In relation to the identified problem drivers, the above-mentioned measures are expected to intervene as follows: PM11 & PM12 would allow users of cloud and AI computing services to reliably identify the level of sovereignty of a service. PM15 and PM21 add a sovereignty risk assessment for the public sector to identify its sovereignty needs. These measures directly address PD4 (absence of clarity around the concept of sovereign cloud and AI computing services), with growing degrees of intensity. As European providers of cloud and AI computing services can be considered to be in a good starting position for meeting the benchmark of sovereignty, and because of the public sector's particular interest in relying on sovereign services, these measures also address PD3 (limited public sector uptake of cloud and AI computing services supplied by European providers) – with PM19 and PM21 being the most direct. PD3 refers in particular to the lack of stable contracts for European CSPs, which would be mitigated through PM15 and, more directly, through PM21 and PM19. PM13, PM18, PM23 and PM24 enhance the visibility and usability of services provided by a more diverse set of cloud and AI computing service providers, including European ones. They make it more likely for users, including the public sector, to choose these solutions (meaning a contribution to tackling PD3) and contribute to addressing the factors summarised under PD1 (lack of scale and scope of EU cloud service providers). PM14 contributes to interoperability, thus addressing PD1 (enhanced interoperability is a way of arriving at more integrated service offerings and lower the threshold for users to combine multiple offerings from European providers). PM16 and PM19, allows for the recognition of an EU-added value in public procurement and PM15 and PM21 will shed light on sovereignty vulnerabilities in the public sector, likely to result in a growing turn towards sovereign, including European services and thus addressing PD1 (more public contracts can be expected to help European providers grow the scale and scope of their service offer). PM17 and PM22 will boost public sector uptake, including to the benefit of European providers. They can thus be seen as addressing PD3. PM22 would allow aggregation of demand for innovative solutions, allowing the EU to do what the US has done with a lot of success in the past, i.e. award large contracts which support early innovation and uptake (see PD1). PM20 boosts the public sector's use of/contribution to open source, creating opportunities for smaller players, because open source allows for a faster development of new solutions and allows new ideas to challenge existing market silos. It thus contributes to both PD3 and PD1. PM24 addresses the information imbalance currently affecting the cloud market by allowing for better visibility of smaller providers and comparability across provider ecosystems.

5.2.3. Relationship between policy options and policy measures

Table 7. Overview of the Policy Options and links with the Problems, Problem Drivers, and Specific Objectives

Problem driver(s)		Problem	Policy Option	Policy Measures	Specific objectives*	
PD1	PD2				SO1	SO2
✓		**P1**: Limited and geographically concentrated availability of computing capacity in the EU	**1A:** Enhancing the existing collaborative framework	**PM1**: Expanding the Alliance for Industrial Data, Edge and Cloud with a workgroup on data centres and extending membership to relevant players		✓
✓	✓			**PM2**: Creating a forum for exchanges between relevant public and private stakeholders involved in the buildout of data centres		✓
✓	✓			**PM3:** Adopting guidelines on building sustainable data centres in the EU	✓	✓
✓	✓		**1B:** Legislative and financial intervention enforced nationally	**PM4:** National facilitator for data centre projects		✓
✓	✓			**PM5:** Mechanism for Member States to identify areas for fast-track data centre deployment	✓	✓
✓	✓			**PM6:** Possibility for public support for data centres	✓	✓
	✓			**PM7:** Set deployment targets and monitor progress	✓	
✓	✓		**1C:** Legislative and financial intervention enforced at EU level	**PM8:** EU R&D funding	✓	
✓	✓			**PM9:** EU deployment funding for strategic projects	✓	✓
✓	✓			**PM10:** EU-level identification of areas for fast-track data centre deployment	✓	✓

* **SO1**: Increase computing capacity deployed in the EU through innovative and sustainable technologies
SO2: Ensure attractive conditions for the deployment of sustainable and innovative computing capacity
PD1: Lack of scale and scope of European cloud and AI computing service providers
PD2: Bottlenecks slowing down data centre expansion

Problem driver(s)			Problem	Policy Option	Policy Measures	Specific objectives*	
PD1	PD3	PD4				SO3	SO4
		✓	**P2**: Dependence on cloud and AI computing services supplied by non-European providers	**2A:** measures to increase transparency and visibility of sovereign cloud and AI computing services	**PM11:** Creating an EU-level harmonized criteria for sovereign cloud and AI computing services	✓	✓
		✓			**PM12:** EU guidelines on the requirements to be fulfilled by sovereign cloud and AI computing service providers	✓	✓
✓		✓			**PM13**: Awareness raising on EU digital sovereignty	✓	✓
✓					**PM14:** Measures for effective interoperability of cloud and AI computing services	✓	
✓	✓	✓		**2B:** Voluntary framework for advancing sovereign cloud and AI computing services	**PM15**: Voluntary sovereign risk assessments for the use of cloud and AI computing services in the public sector	✓	✓
✓	✓				**PM16:** Voluntary award criteria rewarding a European added value	✓	✓
	✓				**PM17:** Public sector cloud federation and EU broker		✓
✓	✓				**PM18:** Creating vendor-neutral cloud and AI training	✓	
✓	✓			**2C:** EU-coordinated procurement and support framework for sovereign cloud and AI computing services	**PM19**: Mandatory specific award criteria for the procurement of cloud and AI computing services	✓	
✓	✓				**PM20:** Boosting open source use in and by public administrations	✓	✓
✓	✓	✓			**PM21:** Mandatory sovereignty risk assessment for the procurement of cloud and AI computing services	✓	✓
✓	✓				**PM22:** Joint EU-level public procurement of cloud and AI computing services	✓	✓
✓					**PM23:** SME cloud and AI support scheme	✓	
✓					**PM24**: Cloud and AI toolbox	✓	

*__SO3:__ Decrease the overall reliance on non-European cloud and AI computing service providers
SO4: Contribute to the protection of public order by enhancing the resilience of supply of cloud and AI computing services, in particular in the public sector
PD1: Lack of scale and scope of European cloud and AI computing service providers
PD3: Limited public sector uptake of cloud and AI computing services supplied by European providers

PD4: Absence of clarity around the concept of sovereign cloud and AI computing services

5.2.4. Relationship between Problem Drivers and Policy Measures

Table 8. Aspects of the Problem Drivers addressed by the Policy Measures

	PD1: Lack of scale and scope of EU CSPs	PD2: Bottlenecks slowing down data centre expansion	PD3: Limited public sector uptake of cloud and AI computing services supplied by European providers and diverging procurement practices	PD4: Absence of clarity around the concept of sovereign cloud and AI computing services
PM1 - Cloud Alliance expansion	*Improved networking between colocation operators and European CSPs*			
PM2 - Data Centre Forum		*Identification of suitable land; improved administrative awareness for individual DC projects; improved awareness for electricity grid needs*		
PM3 - Data Centre guidelines	*Easier access to best practices by smaller scale operators*	*Identification of suitable land; best practices on fast deployment*		
PM4 - National facilitator	*Being accompanied through administrative processes is of particular benefit to smaller, including European, CSPs*	*Acceleration of administrative processes; making regulatory environment easier to navigate*		
PM5 - Fast-track areas	*Smaller scale operators stand to benefit proportionally more from accelerated administrative processes*	*Identification of suitable land; acceleration of administrative processes; making regulatory environment easier to navigate*		
PM6 - National funding support	*Lowering the infrastructure entry barrier*	*Access to capital*		
PM7 - Deployment targets		*Recognition of strategic importance*		
PM8 - EU R&D funding	*Lowering the infrastructure/innovation entry barrier*	*Access to capital*		

	PD1: Lack of scale and scope of EU CSPs	PD2: Bottlenecks slowing down data centre expansion	PD3: Limited public sector uptake of cloud and AI computing services supplied by European providers and diverging procurement practices	PD4: Absence of clarity around the concept of sovereign cloud and AI computing services
PM9 - EU deployment funding for strategic projects	*Lowering the infrastructure entry barrier*	*Access to capital*		
PM10 - EU-level fast-track	*Smaller scale operators stand to benefit proportionally more from accelerated administrative processes*	*Identification of suitable land; acceleration of administrative processes; making regulatory environment easier to navigate*		
PM11 - EU-level harmonized criteria for sovereign cloud and AI computing services				*Improved identification of sovereign services*
PM12 – EU guidelines on requirements to be fulfilled by sovereign cloud and AI computing services				*Improved identification of sovereign services*
PM13 – Awareness raising on EU Digital Sovereignty	*Enhanced visibility and drive uptake of sovereign, including European, CSPs*			*Improved identification and visibility of sovereign services*
PM14 – Interoperability flanking measures	*Improved opportunities for building integrated offers*			
PM15 – Voluntary sovereign risk assessments for the use of cloud and AI computing services in the public sector	*Improved commercial opportunities for providers of sovereign services, including Europeans*		*Recommended uptake of sovereign services, including those provided by European CSPs, for highly critical use cases*	*Improved identification and visibility of sovereign services*
PM16 – Voluntary award criteria	*Improved commercial opportunities for providers from the EU (and countries with which the EU has no dependency)*		*Facilitated access to EU providers (and from countries with which the EU has no dependency)*	
PM17 – Public sector cloud			*Boosts uptake*	

	PD1: Lack of scale and scope of EU CSPs	PD2: Bottlenecks slowing down data centre expansion	PD3: Limited public sector uptake of cloud and AI computing services supplied by European providers and diverging procurement practices	PD4: Absence of clarity around the concept of sovereign cloud and AI computing services
federation and EU broker				
PM18 – Vendor-neutral cloud and AI training programme	*Increased likelihood of uptake of services provided by smaller CSPs*		Upskilled workforce increases likelihood of switching	
PM19 – Mandatory award criteria	*Improved commercial opportunities for providers from the EU and countries with which the EU has no dependency*		*Facilitated access to EU providers (and from countries with which the EU has no dependency)*	
PM20 – Open Source use in the public sector	*Creates opportunities for smaller providers*		*Boosts uptake*	
PM21 – Mandatory sovereign risk assessments for the use of cloud and AI computing services	*Improved commercial opportunities for providers of sovereign services, including Europeans*		*Mandatory uptake of sovereign services, including those provided by European CSPs*	*Improved identification and visibility of sovereign services*
PM22 – Joint EU-level procurement of cloud and AI	*Enhanced possibilities for large contracts supporting early innovation and uptake*		*Boosts uptake*	
PM23 – SME cloud and AI support scheme	*Enhanced commercial opportunities for SME providers, including Europeans*			
PM24 – Cloud and AI toolbox	*Enhanced visibility and comparability, including for European providers*			

5.3. Options discarded at an early stage

- Mandating the digitalisation of permitting processes for DCs throughout the EU. While the Inter-institutional Better Regulation encourages to consider the digitalisation of processes when defining policies, digitalising the permitting process is intuitively perceived as something better tackled in a horizontal measure covering the whole spectrum of industrial installations rather than through a sectoral basis.
- Introducing measures on tackling the lack of grid capacity: As the issue with the lack of available grids capacity in certain locations is not unique to DCs, and grid access is regulated by energy legislation, option introducing sector specific measures to tackle lack of grid capacity was discarded. Ensuring grids will be in place and ready to uptake future loads is dealt by on a horizontal level under the European Grids package.
- Options to directly improve the availability of private capital have been discarded. First, because the policy measures under PO1-A/B/C, by simplifying and accelerating the deployment of DCs, are already conducive to an improved investment landscape.
- Creation of a national central and public repository where Member States can include all relevant information on areas designated for DC deployment. This option is discarded as it would favour real estate speculation and overall bring little benefit for DC investors.
- Common Procurement Vocabulary (CPV) i.e. standardised tender vocabulary at EU-level for procuring cloud and AI computing services for a more precise monitoring of public sector capacity and demand. The existing CPV codes do not include a specific entry for cloud and AI computing services and are instead classified as ICT services or ICT infrastructure. This option is discarded as adding such a code would require a full re-think of the codes related to the procurement of ICT in general, something that is beyond the scope of this intervention.
- The set up of an agency to implement several of the PMs laid down in this assessment, such as the operating the coordination hub from PM5, operating the broker from PM17, conducting the procurements from PM22 or running the marketplace from PM24. This option was discarded at an early stage as perceived as institutionally difficult to deliver.
- In the context of PM15/21, reverse the logic of the sovereignty framework where it would fall on contracting authorities to trigger sovereignty audits in the context of public tenders and only if a similar service is not already audited (as currently the case under FedRAMP). This option has been discarded as it would limit the number of services under levels 2, 3 or 4, at least initially, and create an artificial barrier for providers to have their services assessed against the sovereignty framework. It also delays procurement procedures where a new service needs to go through the whole evaluation process.

5.4. Possible combination of options

As discussed above, the first set of PMs are grouped by their regulatory nature and governance level, i.e. non-regulatory vs regulatory and national vs EU action. **PO1-A** focuses only on soft, non-regulatory instruments, whereas **PO1-B** and **PO1-C** are of a regulatory nature, enforced at national and EU level respectively. As such, some combinations of measures are mutually exclusive, e.g. PM4 and PM5 (national regulation under PO1-B) cannot coexist with PM10 (EU-level regulation under PO1-C) as they address at different levels the bottlenecks to expand DC capacity in the EU. However, other measures under PO1-B and PO1-C can be complementary, for example potential public support for DCs (PM6) could align with EU-level instruments, such as those under PM8 and PM9, creating a multi-level financing framework to addresses a critical dependency from the EU. Similarly, all or selected elements of PO1-A (e.g. guidelines, forum) could be combined with either PO1-B or PO1-C to enhance regulatory action with soft support.

The deployment targets to monitor the expansion of capacity in the EU under PM7 could also be adopted independently of PO1-B, either in combination with PO1-A, PO1-C or in the context of the forthcoming review of the Digital Decade Policy Programme.

By contrast, **PO2-A/B/C** follow a deliberately incremental approach to intervention along sovereignty and federation of public resources (see section 5 and annex 4 for details). The related PMs are not designed to be combined with one another, but rather reflect the degree of intervention, with the higher levels of intervention building on the mechanisms established in the preceding one. As best visualised in the graph at the end of section 5.2.2, PM15 builds on PM11; in turn, PM21 builds on PM15. PM19 builds on PM16. Similarly, PM22 builds on PM17. Finally, PM23 has clear synergies with PM18. The remaining PMs, i.e. PM12, PM13 and PM14 under PO2-A are stand-alone measures that could be retained independently

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section summarises the main expected economic, social and environmental impacts of each Policy Option (PO) compared to the baseline. The assessment draws on multiple data sources, including stakeholder consultations (interviews and surveys) and desk research in the context of the supporting study. To the extent possible, the impacts are quantified based on available assessments or modelling. Where dedicated modelling/monetisation was not possible due to the lack of data, a qualitative assessment was performed, drawing on existing studies and input from stakeholders, to ensure transparency on the full range of potential effects. A sensitivity analysis is provided in section 7.5 to indicate the potential range of error and uncertainty for selected key estimates. Where central values were not sufficiently informative, or relied on an excessive number of assumptions, illustrative ranges are provided to inform of the expected consequences and impacts of the proposed measures. Annexes 3, 4 and 12 provide further details on the methodological approach, detailed tables and estimates.

In addition, it is worth mentioning that this assessment found practical experience in the public procurement for sovereign cloud services conducted by the European Commission. The tender was launched in October 2025, as part of Commission's efforts to strengthen the digital sovereignty posture of the European Union Interinstitutional Bodies and Agencies. Even though they exist in different contexts, the sovereign non price award criteria used in the tender has some resemblance to the proposed sovereignty framework in PM15/PM21[102].

6.1. Economic impact

This section describes first the expected direct, quantifiable economic impact of the policy options on key identified stakeholders, i.e. industry, including SMEs, public authorities, and the European Commission. As part of the analysis, an assessment of wider economic effects is then provided, including impacts on innovation and technological sovereignty. This impact is assessed mainly based on literature, desk research and stakeholder evidence.

6.1.1. Impact on industry, including SMEs and private sector essential entities

The impact of the policy options on **industry** was assessed based on the quantifiable expected costs and benefits for key business stakeholders. First, improving the availability of computing capacity in PO1-A, PO1-B, PO1-C, directly impacts **DC operators** and other enterprises building DCs. Second, reducing the dependence on cloud and AI computing services provided by non-EU

[102] In the Commission tender, the non-price award criteria included a number of 'sovereignty' criteria against which tenders were scored by the evaluation committee. In PM15 and PM21, the harmonised sovereignty criteria are assessed by a third party auditor and subsequently verified by a public authority. This leads the service to obtaining a label which is necessary to participate to call for tenders where the contracting authority does not need to look again into the sovereignty aspects of the service (but can still request information).

cloud and AI service providers in PO2-A, PO2-B, PO2-C, is expected to have a direct impact on **cloud and AI computing service providers, on the public sector and on private sector essential entities in accordance to Annex I of NIS2**. This section outlines the quantifiable and expected direct costs and benefits for these stakeholders in present value over the next 10 years, while section 6.1.5 presents the anticipated wider economic effects that the proposed measures could have. The detailed explanations for the assumptions behind these estimates can be found in Annex 4, sections 2 and 3[103].

Adjustment and administrative costs for data centre operators. **PO1-A** would only foresee adjustment costs for DC operators' stemming from their participation in the new Alliance Working Group (PM1), forum for exchanges (PM2) and from their potential uptake and discussion of the guidelines on building sustainable DCs (PM3). These costs have been estimated as ranging between **EUR 8-18 m**. Under **PO1-B,** 400 estimated DC operators and CSPs active in building data centres are expected to face one-off administrative costs to comply with the conditions to access fast-track areas (PM5), i.e. preparing the application file, completing standardised templates and submitting evidence of compliance with areas conditions. The total costs for this activity are estimated between **EUR 1-3 m** at present value over 10-years. Operators are also expected to face adjustment costs to adapt new projects for DC build out and comply with the related requirements. These adjustment costs are estimated to be approximately between EUR 6 and 26 m for these stakeholders over the assessment period. The participation in a potential funding scheme under PM6 would also generate administrative costs to account for the staff time spent on preparing applications to benefit from funding. Under PM7, businesses would face minor administrative costs to respond to surveys and/or provide additional information for reporting on DC capacity. Total costs under this option for data centre operators are thus estimated between **EUR 7 and 31 m**. Under **PO1-C**, similar activities would occur at EU level. Companies participating in EU funding programmes (PM8, PM9) would face administrative costs for preparing and managing proposals. 20 proposals every two years have been estimated for such purposes, leading to costs ranging between EUR 1 and 3 m. As in PO1-B, providers would also be expected to face both administrative and adjustment costs to access the areas and benefit from accelerated DC deployment under PM10. These costs have been estimated to range between EUR 5 and 25 m, catering for some uncertainty in the effort dedicated to such administrative and adjustment activities. The total value of costs for DC operators and CSPs active in building data centres are thus estimated to range between **EUR 7 and 27 m** under this option (discounted values over the 10-year assessment period).

Adjustment and administrative costs for cloud and AI computing service providers. Under **PO2-A**, cloud and AI computing service providers would face adjustment costs, estimated as additional effort to discuss the new guidelines (PM12), participating to the annual conference (PM13) and in setting up and participating to the coordination group for standards development (PM14). These activities are expected to generate total costs for providers ranging between **EUR 16 and 19 m**. Most of these costs would derive from PM13, where 300 participants have been accounted for. Under **PO2-B**, recurrent adjustment costs for providers would emerge mainly from complying voluntarily with the sovereignty risk assessment framework (PM15). These are estimated at service level because the audit procedure would apply to individual cloud and AI computing services, i.e. providers incur costs for each service that undergoes an audit. These costs emerge

[103] For readability purposes, direct administrative and adjustment costs and corresponding direct savings or economic benefits are merged, in the following sections but are further detailed in Annex 4 and broken down by cost type (one-off or recurrent). The policy options are assumed to be implemented from 2027 onwards, with the quantitative assessment covering the 2027-2036 period for the EU and all figures expressed in real 2025 euros.

from the one-off effort required to meet the necessary legal, organisational and technical conditions to reach the sovereignty assurance levels 2-4, undergo third-party audit, and pay audit and renewal fees. Recurrent audit-related administrative costs are also expected in subsequent years. Moreover, EU-based cloud and AI computing service providers are expected to incur one-off adjustment costs to comply with the non-price award criteria (PM16), e.g. rewarding EU-based R&D&I for innovative services, by altering their systems and processes to be able to participate in public procurement procedures. Additional administrative costs have been estimated as providers prepare their bids. Summing these costs leads to total costs ranging from **EUR 67 m to EUR 160 m**. Under **PO2-C,** the measures are estimated to generate similar administrative and adjustment costs for providers as PO2-B, but more services (600 compared to 150 in PO2-B) are expected to undergo third-party audits to participate in public procurement procedures (PM21). This leads to higher costs for cloud and AI service providers across the EU that are estimated to range between **EUR 233 and EUR 484 m**. As above, these adjustment costs are personnel related, i.e. the effort needed to modify the providers' policies and procedures and adjust the legal and organisational safeguards to be able to meet the criteria under sovereignty assurance levels 2-4.

On top of this, private sector essential entities identified under Annex 1 of NIS2 would have to incur administrative costs to include non-technical risks in their risk assessments, i.e. adding sovereignty elements on their existing risk assessment activities. These costs could range between **EUR 486 m and 2.6 bn,** i.e. corresponding to the effort required per entity (from a minimum of 20 to a maximum of 110 days) and taking into account 25 600 private entities operating in sectors of high criticality across the EU.

Focus box #1: costs for service providers to develop sovereign services

Assessing the cost and benefits for providers to provide sovereign services is a complex task that involves many parameters and differs greatly from provider to provider. As well, in the absence of an established market for sovereign services, data sources are rather anchored in providers' business plans, not in ex post analysis of established businesses. Such data is confidential to companies, and the below considerations are based on targeted discussions with stakeholders that requested to remain anonymous. A first consideration is that the consulted companies unanimously indicated that, in developing the business plan for these new services, they count on new large critical use cases that are today not in the cloud; in other words, they see sovereign services to generate a new source of income, but not to substitute existing.

Cost wise, new costs notably include the amortisation of all one-off adjustment costs such as the additional cost induced by using EU-located infrastructure, the additional compliance costs induced by the audits, the additional costs of being certified under EUCS; and proper recurrent costs such as the higher salaries of employing EU workforce.

As an illustration, speaking under the condition of anonymity for business secrecy reasons, an EU service provider specialised in sovereign services speaks of an overall investment of EUR 1.5 bn, including hardware, for a broad range of IaaS and PaaS services (for an unspecified computing capacity).

Conversely, another EU service provider with an established range of non-sovereign services speaks of an overall investment in the range of EUR 20-40 m to adjust existing hardware and software to the stricter norms that a sovereign service entails, with plans to invest progressively should the market develops.

The benefits for service providers to develop sovereign services are covered under section 6.1.5.

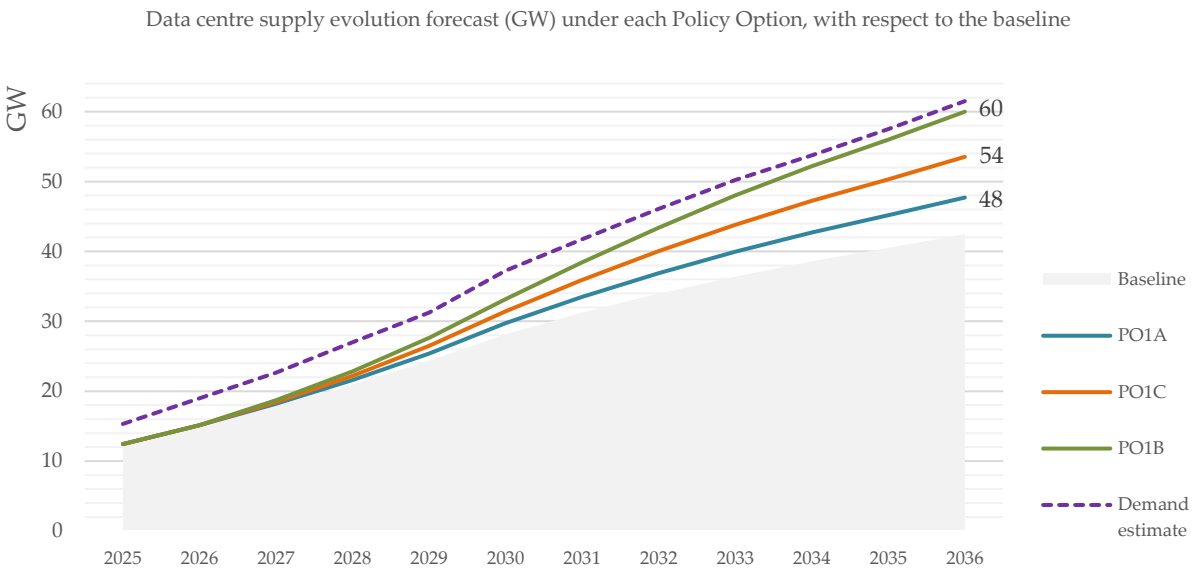
Economic benefits and cost savings for data centre operators. **PO1-A** would be expected to generate direct cost savings, via improved information and administrative burden reductions. Although voluntary, the new guidelines (PM3) would contribute to increase clarity, simplify procedures and reduce the incidence of mistakes, saving time for operators during the pre-operation phase of building a new DC, modelled as a central 10-day time saving. When multiplied by the expected number of facilities that could benefit from this time and consequent cost saving, the guidelines would generate discounted savings ranging **between EUR 1 and 3.5 m** over the assessment period. **PO1-B** would bring the largest direct economic impact for DC operators, modelled through a Net Present Value approach which compared the baseline permitting duration with the accelerated scenario to estimate the economic value of bringing constructions and commercial operations of a DC facility forward in time. Based on the evidence collected, the project facilitator for DC roll-out (PM4) combined with access to fast-track areas (PM5) are expected to reduce uncertainty on investment locations by excluding non-viable sites and decrease time to market for DC projects by on average 14 months. Under the baseline scenario, the total time to build a DC, i.e. from planning to entry into operation, was estimated at 32 months on average across the EU. This time is expected to decrease by 6 months from 2027 onwards due to the project facilitator and by an additional 8 months due to streamlined access to fast-track areas[104]. The estimated NPV gain is also associated with the expected reduction in PUE foreseen under this measure, as only the most sustainable DCs would be able to benefit from the fast-tracking. Therefore, the expected improvements in energy efficiency, modelled as a declining PUE, would also contribute to reducing operating costs over time. Over the 10-year assessment, this option could result in discounted economic benefits ranging between **EUR 8 and 27 bn**, considering the uncertainty related to these time savings and their compounded impact on project value. Under **PO1-C**, similar direct economic benefits are foreseen for operators thanks to the EU-level identification of fast-track areas (PM10). Based on discussions with industry and following the validation by the sector in the targeted workshop, these savings are expected to be less consistent than under PO1-B, with an EU-level management of fast-track areas expected to produce time-savings of 3 months. This would in turn still generate consistent economic benefits that would range **between EUR 5 and 12 bn** over the 10-year period.

Figure 10 shows the potential evolution of DC supply under each policy option and the expected reduction in the gap against projected demand in the baseline scenario[105].

[104] Based on study findings and validated by the sector in the targeted workshop.

[105] Annex 4, Section 2.3.3 further explains how the capacity trajectories have been used as the quantitative basis for estimating how many new data centre could be built under each option and the share of this capacity that is expected to benefit from the policy intervention over time.

Figure 10. Forecasted evolution of data centre capacity (GW) under each PO, with respect to the baseline



Source: Technopolis et al. (2025)[106clxv]

Cost savings for cloud and AI computing service providers. Under **PO2-A,** administrative cost savings for providers would mainly stem from the use of the guidelines (PM12), saving time for operators during procurement, modelled as a modest 0.5 days saved per tender procedure, leading to total costs savings that could range between **EUR 2 and 15 m** (10-year, NPV). Under **PO2-B**, providers would face recurrent cost savings from the introduction of a clear and predictable sovereignty risk assessment framework across several Member States (PM15). Instead of responding to different requirements, controls or evidence requests from individual public authorities, service providers would benefit from a common audit procedure and recognised assurance levels with savings ranging from EUR 5 to 16 m per service, under an assumption that the provider operates in 3 to 10 markets. This would reduce duplication and simplify procurement procedures, while reducing costs related to tender documentation. Over time, this is expected to lower compliance costs and make it easier for providers to offer the same audited services to a wider public sector market. This is expected to lead to total benefits for providers ranging between **EUR 200 and 700 m**, when discounted across 10 years. Under **PO2-C**, direct costs savings would stem from the same mechanism explained above, but extended to all MS, and an increased number of services being audited by providers under PM21, compared to PM15, leading to total expected benefits ranging between **EUR 2 and 5.1 bn**, including those savings coming from savings of 1 to 3 working days per bid when drafting specifications by using standard non-specific award criteria (PM19). In the case of PO2-C, savings in the audit process would range from EUR 8 to 25 m per service, assuming each provider run its business in 5 to 15 member states.

Impact on SMEs. Though large businesses dominate the DC, cloud and AI markets, many SMEs in the EU still play a relevant role, particularly providers of cloud and AI services. Thus, the initiative is considered "relevant" for SMEs. Annex 6 contains the SME test. Given the lack of quantitative data, the impact on SMEs is assessed qualitatively below.

PO1-A would generate value for SMEs with improved access to information and clearer frameworks, notably through the guidelines. Early visibility and clarity on applicable requirements

[106] The capacity includes hyperscalers and colocation providers, but not enterprise DCs in the private or public sector.

and collective voicing of SMEs would reduce costs linked to information asymmetries and coordination failures. As smaller operators, SMEs are disproportionately affected by complex permitting procedures and would benefit from administrative simplification. In **PO1-B** streamlined procedures are expected to reduce legal and consultancy expenses and would accelerate timelines, lowering entry barriers, reducing administrative costs and opening opportunities for SMEs in the DC value chain. The impacts of **PO1-C** on SMEs align to those of PO1-B, though EU-level approval might be perceived as more "distant", raising language considerations of such mechanism. In addition, public funding for R&D and innovation would enhance SME participation in advanced projects without requiring large upfront capital. Public funding for strategic deployment projects would improve SMEs' access to contracts for large-scale projects, either directly or within a consortium. PO2 would impact SMEs as providers of cloud and AI computing services, but also as consumers of these services. Under **PO2-A**, the non-prescriptive EU criteria of sovereign cloud and AI computing services and the guidelines would reduce administrative burdens on SMEs while increasing clarity and transparency for sovereign services. The annual conference on EU digital sovereignty would allow SMEs to showcase their services and raise concerns collectively at lower costs. SMEs would also be the greatest beneficiaries of the interoperability measures as it simplifies the re-use of existing technology they lack. Under **PO2-B**, the sovereignty audit procedure with validity throughout the EU would reduce verification costs, especially for SMEs offering their services in critical sectors to public administrations in different Member States, albeit facing more burdensome compliance costs, voluntary public procurement criteria favouring specific characteristics could boost SME participation. Additionally, a vendor-neutral training would provide SMEs with a highly qualified workforce, capable of using and developing advanced cloud and AI solutions. **PO2-C** would entail the greatest direct and indirect net benefits for SMEs. The validity of audit reports across the EU would allow SMEs' services would allow them to extend their commercial offers otherwise hindered. Beyond, remaining costs include funding programmes participation, which is also expected to enhance SMEs' competitiveness. Open source access would reduce entry barriers, where solutions are evaluated on their merits. Encouraging open source would not disadvantage proprietary solutions where these genuinely represent the option on the best-value for money, but this would need to be properly demonstrated. Similarly, for companies, notably SMEs whose business models are built around the delivery of open source solutions and related services, this measure would provide them with the opportunity to present their solutions on equal terms removing barriers that have historically limited open source participation in public procurement procedures.Similarly, financial support would include improved funding rates for SMEs, and the service toolbox would help smaller providers find complementary solutions to their service offering. Ultimately, this would foster SMEs' access to innovation, seeking to increase their competitiveness and reduce their upfront costs. The SME cloud and AI adoption scheme would bring direct economic gains for SMEs applying cloud and AI technologies through improved competitiveness, and indirect gains for IT SMEs offering consultancy, reinforcing the ecosystem to drive a broader SME digital transformation.

SMEs' views on Policy Measures. Feedback from the public consultation shows the following:

Table 9. SMEs and large companies views on Policy Measures

Measure	*Support from SMEs**	*Support from large companies***
Criterion ensuring sovereignty, autonomy, resilience for administrations procuring cloud and AI computing services	88%	31%
Supporting an open source software ecosystem	82%	55%
Guidelines with standard criteria to procure cloud and AI computing services for public administrations	82%	39%

Measure	*Support from SMEs**	*Support from large companies***
Tax incentives for using sustainable technologies	76%	39%
Funding for R&D of energy-efficient technologies, standardised energy efficiency benchmarks; addressing energy availability for data centres	71%	59%
Expedited approval mechanisms and clear conditions for strategic projects	70%	81%

*17 SMEs replied to the public consultation questionnaire
** 49 Large companies replied to the public consultation questionnaire

6.1.2. Impact on public authorities

Costs for public authorities. In **PO1-A,** costs for authorities are estimated to be modest and would be limited to their participation in the forum (PM2) as well as to their contribution to drafting the guidelines (PM3), leading to total expected costs ranging between **EUR 1 and 2 m** over 10 years, assuming one authority representative per MS would participate in each activity. Under **PO1-B,** authorities are expected to face adjustment and administrative costs to establish and operate the project facilitator (PM4)[107] and identify areas for fast-track deployment as part of their national strategies for data centre deployment (PM5). This would lead to an estimated cumulative cost over 10-years ranging between 4 and 8 m per national authority. Additional costs are estimated for setting up and managing a potential support programme for strategic DC roll-out (PM6). Finally, authorities would face minor enforcement costs for periodic checks to verify data on compute capacity as well as the implementation of national data centre strategies under PM7. The option is expected to generate total costs for 27 national authorities ranging between **EUR 106 m and 236 m over ten years**. In **PO1-C,** authorities are expected to incur adjustment costs to adapt to the EU-level DC fast track platform (PM10), including the appointment of national representatives to the new board and periodic provision of data for identifying suitable fast-track areas. This is expected to generate costs ranging between **EUR 84 and 90 m over ten years**. Under **PO2-A**, the measures would generate modest adjustment costs for national authorities. The EU-level criteria of sovereign cloud and AI computing services (PM11) are expected to generate adjustment costs related to the review of national procurement templates, while guidelines (PM12) are expected to generate costs in relation to their adoption and prior consultation process. This would lead to total expected costs for authorities ranging from **EUR 14 to 15 m** in discounted terms over 10 years. Under **PO2-B**, authorities would face increasing costs regarding the sovereignty risk assessment scheme (PM15), the award criteria (PM16), participation in the public sector cloud federation (PM17). First, authorities would face one-off adjustment costs to carry out the sovereignty risk assessment to map sovereignty assurance levels to cloud and AI computing services used in the public sector. They would face recurrent costs for their periodic renewals and for revision of the audit reports (PM15). These are relatively modest and estimated in a range of **EUR 25 to 99 m**. Under this measure, contracting authorities could consider using the sovereignty framework for their procurement decisions. See the box below for the assessment of the potential costs for public authorities related to porting and migrating cloud services. Under this option, since the measure is not mandatory, a smaller group of public authorities has been considered to use the sovereignty framework. The intervention could accelerate the porting of a limited subset of critical cloud applications to sovereign levels 3-4. Based on this, the anticipated porting is assumed to concern only between 1% and 6% of the relevant application base, resulting in discounted costs ranging from **EUR 620 m to EUR 4 bn,** over three years from 2030**.** Minor costs are estimated for

[107] This estimate represents a worst case scenario in which authorities would need to establish a dedicated team from scratch, whereas in practice Member States may rely on existing resources under the Gigabit Infrastructure Act, including by designating a single information point established under Regulation (EU) 2024/1309, with the relevant functions, procedures and mechanisms applying accordingly.

authorities voluntarily updating their procurement templates with the new procurement criteria (PM16). The platform for public sector cloud federation is expected to generate the costs ranging between **EUR 170 to 260 m** in discounted terms. Summing all these activities leads to total costs under this option to range between **EUR 820 m and 4.4 bn**. **PO2-C** foresees costs previously described but scaled upwards as well as new ones. For the former, elements include both the one-off and recurring costs for the sovereignty risk assessment scheme, reflecting the higher number of public authorities that would perform them compared with PM15. Under PM15, around 150 audited services are expected to be verified by 2036, while under the mandatory approach in PM21 this figure is projected to rise to 600 in the same period, which is broadly consistent with benchmarks such as FedRAMP. Also, in the case of PM15, given the voluntary nature of the scheme, only a limited number of Member States would perform the risk assessment and the consequent verification of audited services. Under this option, the mandatory nature of PM21 assumes that all MS would prepare the personnel and the infrastructure to run the scheme. Hence, the changes of PM15 and PM21 would need to be seen in combination: increase in the number of authorities adapting their processes to perform the sovereignty risk assessment and an increase in the number of audit reports to be verified. Therefore, under this option, the cost for authorities assumes that the policy intervention would accelerate the porting of the limited subset of critical applications across the full population of 6 400 public entities considered in scope. This would result in total discounted costs of around **EUR 3 to 15 bn,** over the same period. Under PM19, authorities would also face some costs to update their procurement templates with the new procurement criteria, alongside minor effort to draft an action plan or light touch strategic note outlining how they intend to use public procurement to increase the uptake of highly innovative cloud and AI computing services. PM20, which aims to boost open source in public administrations is expected to produce several costs for public authorities, i.e. related to (i) the creation and maintenance of the Open Source Programme Offices (OSPOs), (ii) setting up open source repositories and governance mechanisms defining contribution, review, and acceptance procedures, (iii) the continuous maintenance and set-up of additional repositories, (iv) the activities needed to release code as open source and (v) the comparative assessments of proprietary and open source solutions for their procurement procedures. While currently public authorities may not have this knowledge in-house, the initial comparative assessments and the set-up of the repositories may require certain investment in staff training and in the development of training evaluation capacity in the contracting authorities. However, these administrative costs are expected to be mitigated thanks to the deployment of the Open Source Programme Offices (OSPO). OSPOs, as part of their role in their technical, legal, procedural and strategic – related tasks, may provide contracting authorities with standardised evaluation frameworks, scoring methodologies or advisory support thereby sharing expertise costs across the public sector rather than requiring each authority to develop this capacity independently. Finally, in PM22 for the public sector cloud federation, national public authorities will have the same costs as described for PM17 above, as it builds on top of it. These measures would result in total costs for public authorities amounting to a range of **EUR 4 to 18 bn** for this option.

Focus box #2: costs for authorities to port and migrate services

This box makes the distinction in between:

- Cloud **porting**, i.e. moving a service from one cloud provider to another cloud provider
- Cloud **migrating**, i.e. moving a service from on-premises to cloud

None of the proposed policy measures obliges public authorities to port an existing cloud service from one provider to another, or to migrate on-premises service to the cloud or to port. These decisions are made on a **case-by-case basis** by public authorities alone, considering the authority's

specific needs, existing systems, and procurement cycle.

Examining costs is however relevant since the results of Member States' sovereignty risk assessments are expected to induce cloud porting decisions[108]. As well, the expected increase in trust resulting from the existence of a sovereignty framework is expected to increase or anticipate cloud migration decisions. These costs are not immediate consequences of the intervention's entry into force, but rather potential future expenses that may arise during the normal course of business. These costs are thus presented for illustrative purposes.

Porting an existing workload from one cloud provider to another (cloud-to-sovereign cloud)

Porting refers to moving an existing cloud-based service from one cloud provider to another, in this case to a sovereign cloud service. This concerns services that are already cloudified but may need to be moved/ported if sovereignty risk assessments conclude so. It is worth noting that this is something that anyway happens naturally as existing contracts come to an end and are re-tendered. To port an existing service, costs include a feasibility assessment, strategy and planning, target environment setup, migration, testing and validation, cutover, DNS switching, and recurrent activities linked to operating the service in the new environment, including performance optimisation and maintenance. These activities mainly involve personnel costs and parallel running costs.

It is important to underline that the cost of porting is comparable when systems are ported from one cloud providers to another or to a sovereign cloud environment. In other words: the fact that the end cloud is sovereign does not per se affect the cost of porting.

The porting of a single system

To estimate the cost of porting an IT system, applications can be grouped into small, medium-sized and large, based on their size, complexity, business case and infrastructure needs. Annex 12 provides an in-depth analysis of the cost categories and their magnitudes, which can be grouped in the following categories:

Application type	Indicative effort	Estimated cost
Small application	50 days	EUR 20 000 – 50 000
Medium-sized application	400 days	EUR 200 000
Large application	1000 days	EUR 500 000

Real-life use case 1: a porting of a high usage application to a sovereign PaaS

One real-life example concerns the porting of an existing application from a cloud to a sovereign Platform-as-a-Service environment.

- In the current situation, the service costs approximately EUR 2 m per year with a large commercial cloud provider.
- The target scenario is porting the application to a sovereign PaaS environment.
- The application is a monolithic Laravel application with a large-scale MySQL database and several large Elasticsearch clusters.
- It does not process or store personal data, but it has a high usage profile, with sustained traffic and high-intensity connections.
- Its criticality is mainly reputational, as an incident could have a high public impact,

[108]It must be noted that porting can also be triggered naturally as a consequence of regular procurement decisions after the expiration of cloud service contracts.

although the service is not considered real-time critical from a business continuity perspective.

The estimated transition effort is around 2 FTEs over six months, broken down as follows:

Workstream	Estimated cost
Application adaptation, migration and validation	1 FTE
Infrastructure provisioning, platform adaptation and automation	0.5 FTE
Security and compliance alignment	0.5 FTE
Total	**2 FTEs over 6 months**

This example shows that the initial migration requires a structured investment to adapt the application, infrastructure and security posture to a sovereign environment. However, part of this effort can be reusable for future migrations, particularly infrastructure patterns, deployment practices and security baselines. The learning curve is therefore front-loaded, meaning that subsequent migrations of similar systems could benefit from the developed experience and skills. The actual effort may vary based on the application's technological stack, its dependence on cloud-specific services and its overall architecture complexity.

Real-life use case 2: transition of an application based on a high-volume database to a sovereign PaaS

Another real-life example of a transition of an existing application to a sovereign Platform-as-a-Service environment:

- The application, based on a few tenths of large scale microservices managing a very high-volume document database (1.5 bn records), is hosted by a large commercial cloud provider and is migrated to a sovereign PaaS environment.
- The application is monolithic with a large-scale relational database, WebLogic application server and proprietary monitoring tools.
- It does not store or process personal data, just public documents, but it has a high usage profile, with more than 100 m visits and around 20 m documents consulted every year.
- Its criticality is mainly reputational, as an incident could have high public visibility, although the service is not considered real-time critical from a business continuity perspective.
- The chosen migration strategy was re-platforming, i.e. migrating the application and the database, and moving from proprietary solutions to open-source solutions (e.g. Apache Tomcat, Postgre SQL, Virtuoso) which entails refactoring code to eliminate dependencies to the deprecated technologies and to align it with the new technological choices, while maintaining the same performance.
- The **estimated transition effort is around 8 000 hours, or 4.5 FTEs over a year.**

What would sovereign cloud porting cost for a typical public authority?

Extrapolating the individual costs of porting different types of applications to the full set of public authorities potentially affected by the policy measures 15 and 21 would require considering several parameters. These include:

- The outcome of the risk assessment with the sovereignty assurance level applicable to the concerned applications
- The number and complexity of IT systems managed by each public authority

- The current level of cloudification of each authority
- Whether the public authority's data are already hosted in the EU under their existing cloud arrangement.

On this basis, three illustrative cases are presented to show how costs can vary across different types of public authorities. These scenarios provide a benchmark for individual authorities, while the aggregated cost across public entities possibly in scope under PO2-B and PO2-C is detailed under Annex 12. The estimates cover the additional anticipated porting of a limited subset of critical applications to levels 3-4 where such porting could be directly accelerated by the intervention.

Small public authority

A small public authority, e.g. a mid-size municipality, manages 200 IT systems, with limited use of cloud services. Around 30% of the systems, i.e. 60, would need to be ported to a sovereign cloud environment. Most of these systems would be small applications (70%), e.g. standard administrative tools, with only limited number of medium (29%) or large platforms (1%). In this scenario, following the risk assessment outcomes, all IT systems (60) are subject to sovereignty requirements, as the authority never considered sovereignty criteria in previous tenders. Most applications (70%) fall under lower sovereignty assurance levels (level 1) while 20% need to be moved to sovereignty level 2 and 10% at least sovereignty level 3. Based on this, the cost of porting for the authority is expected to reach around EUR 4.7-6.0 m over five years, corresponding to around EUR 1 m per year.

Medium public authority

A medium sized public authority, e.g. a national agency, manages around 800 IT systems, with a medium intensity cloud-user profile. Around 30% of its systems are cloudified, i.e. 240, and could be subject to higher sovereignty requirements, i.e. level 2 and above. Based on the outcome of the risk assessment, only 30% of these IT systems would require porting to a sovereign cloud environment, i.e. around 72 systems. Most of these systems are small (60%) or medium applications (37%), with a limited number of large and complex platforms (3%). On this basis, the cost of porting for this authority would reach around EUR 7.3-8.6 m over five years, or around EUR 1.6 m per year.

Large public authority

A large public authority, e.g. a large ministry, manages 1500 IT systems, with intensive use of cloud services, e.g. mission-critical platforms used by citizens, and a higher number of systems subject to sovereignty requirements. Compared to the medium case, it would manage a larger and more complex portfolio, including a larger share of medium (45%) and large (5%) applications. For this scenario, only critical systems falling under Level 2 and above are expected to require porting to a sovereign cloud environment as the authority may already be hosting most of its IT solutions with a cloud service falling under level 1 or on-premises. The cost of porting would reach around EUR 16.6-18.6 m over five years, i.e. around EUR 3.5 m per year.

It is important to distinguish this cost of porting from the price of cloud services, which can be affected by a premium, something discussed under section 2.3.4.

Migration of legacy applications to the cloud

Most public sector use cases are not cloud-based today with 70% estimated to be on-premises. This can be further split, in between 30% that are on premises and could be migrated to the cloud, and a leftover of 40% of on-premises that are legacy applications being phased out (sometimes

long periods of time), or that are too small to deserve particular attention.

To migrate services from **on-premises infrastructure to the cloud**, public authorities face adjustment costs associated mainly with staff time and migration activities. The effort to migrate a legacy-to-cloud application are harder to estimate than the ones for porting because the range of situations is much broader. Annex 12 details them further, leading to an estimate 1.5x the effort compared to porting a service from cloud-to-cloud.

These migration costs need to be put in perspective with the benefits of cloudification. Literature points to potential benefits such as lower infrastructure costs, greater scalability and flexibility, improved service quality, and access to more advanced security and analytical capabilities. These potential benefits are discussed further in Section 6.1.5.

Cost savings for national public authorities. **PO1-A** is expected to realise direct cost savings for authorities in terms of administrative burden reduction from harmonised EU guidelines that would limit divergent interpretations of permitting requirements (PM3), leading to savings that would range between **EUR 0.1 and 0.6 m**, modelled as a 2-day saving per new project adopting the guidelines. Under **PO1-B,** recurrent savings would stem from administrative simplification for DC buildout (PM4), combined with the central mechanism to identify fast-track areas (PM5), which would avoid duplication and back and forth interactions with economic operators, leading to total expected administrative cost savings under this option ranging between **EUR 166 and 277 m**. In **PO1-C**, savings would result from a centralised EU-level structure reducing national efforts (PM10). Consequently, total cost savings for 27 public authorities could be between **6 and 19 m**, based on the variability in the actual effort saved by using a central EU-based database and avoiding repeated clarifications with operators on siting rules. Under **PO2-A**, cost savings are expected to arise from clearer information used in procurement processes. However, the scale of this effect appears to be very limited to be quantified. Under **PO2-B**, the sovereignty scheme and repository (PM15) would help streamline compliance verification by providing information in a single place. Participation in the public sector cloud and AI computing service federation (PM17) is expected to generate considerable resource savings through an optimised use of compute capacity. Finally, the use of standard award criteria (PM16) is also expected to save authorities time in procurement processes, leading to total expected savings ranging between EUR 8 and 17 bn. Under **PO2-C**, cost savings derive from standardisation and automation at scale. Mandating sovereignty risk assessments (PM21) are expected to create a more systematic and trustful manner to assess needs for cloud and AI computing services and reduce their time for procurement thanks to the comfort of having compliance with sovereignty requirements verified ex-ante. Today, there are in several Member States (ex: France, Italy, Finland) some schemes and methodologies used at national level for the overall security and resilience of cloud computing services. Whereas a voluntary approach may not lead to convergence between them, a compulsory system as proposed in this measure, combined with Commission's support and oversight, will have more benefits in terms of synergies between Member States, and will also complement other measures proposed to consolidate efforts. Notably, participation in the public sector cloud and AI computing service federation alongside voluntary EU-level joint procurement (PM22) are expected to generate significant savings through an optimised use of compute capacity, a more cost-efficient procurement and improved economies of scale. Greater use of open source (PM20) is expected to reduce proprietary license expenditures, lowering licensing costs and total cost of ownership for IT systems[clxvi]. These measures could altogether lead to considerable cost savings for authorities ranging **between EUR 21 and 61 bn** over 10 years. A significant part of these savings come from the EU-level joint procurement that starts managing 2% of the total cloud and AI procurement

volume of national contracting authorities reaching 20% at the end of the 10-year period and moving from 10% savings in first year to a range of 20-40% at the end of the period as economies of scale increase.

6.1.3. Impact on the European Commission

Administrative and adjustment costs. **PO1-A** is expected to generate one-off and recurrent administrative costs, regarding the development of guidelines (PM3), the establishment of the new Alliance Working Group (PM1) and DC forum (PM2), leading to modest additional costs with respect to the baseline of around **EUR 0.5 m**. **PO1-B** would entail one-off adjustment costs and recurrent ones for establishing and subsequently managing the coordination hub supporting Member States in identifying fast-track areas (PM5), as well as adjustment effort to monitor and coordinate the monitoring and reporting on computing capacity (PM7), leading to expected total discounted costs over 10-years of around **EUR 1 m**. **PO1-C** would generate the highest economic burden for the Commission, with adjustment costs linked to setting-up and operating the 7-year funding programme for R&D and innovation ecosystems (PM8) and for funding the deployment of strategic projects (PM9). Finally, the EU-level identification of fast-track areas (PM10) would entail one-off adjustment costs to set up the mechanism and procuring a supporting digital tool, along with recurrent costs to manage the mechanism to identify areas for fast-tracked DC deployment and biennial adjustment costs for outsourced studies and expert meetings, leading to total costs of **EUR 17 and 19 m**. **PO2-A** is expected to generate one-off adjustment costs for the Commission from drafting and consultation for the development of an EU-criteria and guidelines on the notion of sovereign cloud and AI computing services (PM12). The annual week-long conference on digital sovereignty (PM13) would also entail recurrent adjustment costs for preparation time and event budget. Finally, the increased standardisation efforts on interoperability (PM14) are expected to generate modest one-off adjustment costs for procuring ad hoc studies and setting up the coordination group, and recurrent costs for participating and supporting discussions. This would lead to total costs of around **EUR 7 m**. Under **PO2-B**, costs are expected to arise from establishing and managing the repository of sovereign services (PM15), setting up the public sector cloud federation platform (PM17), and develop the training programme (PM18). These measures are expected to amount to discounted total costs of approximately **EUR 130 m**. In **PO2-C**, costs for the mandatory sovereignty risk assessment (PM21) would mirror those listed under PO2-B and comprise the procedures for setting up the repository. EU-level procurement (PM22) would generate adjustment costs related to hosting and maintaining the platform, and recurrent ones for operating it for joint procurement. The development, set-up and administration of the adoption scheme for SMEs (PM23) is expected to generate the highest adjustment costs under this option. Finally, the online toolbox for service providers to easily identify software tools to help them in complementing their service offering (PM24) is expected to generate costs related to the development and management of the toolbox. The measures are altogether expected to generate costs for the Commission amounting to in- between **EUR 470 and 760 m** at present value over the next 10 years.

6.1.4. Impact on innovation and technological sovereignty

PO1-A would not expand the supply chain or balance dependencies on non-EU providers. Innovation effects would also be limited. **PO1-B** would be very impactful in terms of technological sovereignty and innovation. The funding of strategic projects would allow national public authorities to steer the development of infrastructure to sectors relevant to sovereignty and to DCs that deploy novel technologies for resource efficiency. **PO1-C** would have a higher innovation impact than PO1-B. Funding the development and deployment of novel technologies

would give an edge to the European DC ecosystem. **PO2-A** would have moderate impact on technological sovereignty. Soft harmonisation measures like defining a sovereign cloud and AI computing services, guidelines, and establishing an annual conference on digital sovereignty would indeed create a common understanding of sovereignty but would have limited impact. The development of harmonised interoperability standards would enhance the uptake of sovereign technologies. **PO2-B** would have greater impact than PO2-A on technological sovereignty in the Union, as the voluntary sovereignty risk assessment would allow public authorities to procure cloud and AI computing services that comply with the sovereignty criteria. The federation would ensure that authorities benefit from de facto sovereign cloud and AI resources shared by other public bodies and would enhance resilience by allowing access to capacity located in other Member States. The voluntary award criteria on R&D investment and supply chain reinforcement are expected to encourage the development of an EU located innovation ecosystem. **PO2-C**, which builds on PO2-B, is expected to have the greatest impact in terms of innovation and technological sovereignty. The sovereignty risk assessments performed by the public and private sectors will improve the overall sovereignty level of the EU economy and will provide additional opportunities and incentives to procure from European providers that are more immune to risks linked notably to data access or throttling of service quality**.** This in turn will encourage investment to improve innovation and technological sovereignty in the EU. The establishment of a framework for joint procurement would allow public authorities to increase their autonomy and resilience while funding innovative solutions in Europe. The non-price award criteria would allow contracting authorities to procure cloud and AI computing services to favour investment in innovative cloud and AI computing services, while reducing critical dependencies. The open source principles would also play a role in the increase of the Union's operational autonomy, particularly in the public sector. Finally, the toolbox for cloud and AI computing service would support European cloud and AI computing service providers in complementing their service offerings and increasing their market visibility, by addressing fragmentation and lack of discoverability in the cloud market. Therefore, the toolbox is expected to contribute to reducing dependency on a limited number of dominant solutions.

6.1.5. Wider economic effects

Beyond the direct costs and benefits quantified above, the proposed measures may generate wider economic effects through two main channels: first, support the deployment of data centres, with a focus on strategic ones prioritising innovation and sustainability, and second, by increasing the adoption of sovereign cloud and AI computing services. These effects are difficult to quantify because they relate to resilience, autonomy, avoided disruption and long-term competitiveness. However, given their economic relevance, the main evidence collected is summarised here as part of the overall assessment.

Compute Capacity. The overall macroeconomic impact of constructing new data centres is best analysed qualitatively. The evidence base remains fragmented in part because official statistics often fail to categorise data centres as a distinct sector, and in part because several studies rely on project-specific case studies, surveys or modelling that cannot be scaled to the whole European context without large multipliers. Existing literature suggests that **the construction and deployment of new data centres have a positive impact on the economy in the short to medium term**. The development of new data centre projects generates demand for various goods and services, including construction, engineering, electrical equipment and professional services. These in turn can have ripple effects on local economies through related supply-chains and induced household spending. However, the extent of these effects is heavily influenced by local procurement patterns, labour market conditions, and degree to which these expenditures are

retained domestically. Studies indicate that investing in additional data centre capacity can stimulate economic activity during the construction phase, but the magnitude of this effect depends on the specific context[109]. Some have attempted to quantify the contribution of data centres to GDP or value added. For example, in the UK, it has been estimated that the data centre sector generates around GBP 4.7 bn in annual Gross Value Added. Similarly, a 2025 study by Copenhagen Economics estimates that in Portugal the data centre sector contributed EUR 311 m to GDP between 2022 and 2024, with potential cumulative contributions ranging from EUR 6.1 bn to EUR 26.2 bn between 2025 and 2030, depending on the investment scenario[110].

When looking at international trade, expanding EU DC capacity is also expected to affect the EU's external trade balance by **increasing imports of semiconductors and ICT components**. Today, Europe has a structural import dependency on semiconductors and the most advanced AI chips used in DCs are designed and fabricated outside the EU, mainly in the US, Taiwan, South Korea and China[clxvii]. Each new GW of installed capacity requires several millions of components, representing between EUR 3 to 4 bn of ICT hardware expenditure per GW[clxviii]. Applying this ratio to the EU's projected 2025-2030 buildout, total chip and server imports could reach EUR 47 to 83 bn over this period. This dependency is expected to further catalyse foreign direct investment (FDI) and technology upgrades within the EU, with technology firms potentially contributing to the development of clusters around the growing DC sector[clxix]. At EU level, in 2024, investors announced FDI projects worth around EUR 60 bn[clxx].

From a broader economic perspective, the development of additional compute capacity serves as an **important enabler for cloud computing, AI and other data-intensive activities**. The primary economic benefit is likely to arise from the downstream **effects on productivity and innovation**, rather than the construction and operation of the data centres themselves. This in turn can have a positive impact of the economy by supporting growth and regional digital development. According to the OECD, cloud services play a key role in the value chain for many digital technologies used by businesses and governments, and can **enhance innovation and productivity, particularly for SMEs** that would otherwise face high fixed costs in acquiring advanced ICT capacity[clxxi]. Scalable and secure compute and cloud-based services can empower enterprises and public authorities to access advanced technologies without having to build the infrastructure in-house, something which requires time, a particular skill set and large upfront investments. Better access to digital infrastructure can improve the conditions for technology diffusion and digitalisation across sectors, ultimately giving rise to data-driven business models, including AI-enabled services. In the EU context, this is consistent with the policy objective of ensuring that strategic data centre capacity supports public interest use cases, such as healthcare, public administration, research, security, critical infrastructure and AI-enabled public services. The ultimate benefit of fostering this deployment would reside not in the creation of more data centres, but in the availability of **strategically located and appropriately governed compute capacity for economically and socially important workloads**. As noted above in Section 2.2.1, the availability of local data centre access can also have an impact on latency, reliability and cost conditions, which can encourage greater cloud adoption[clxxii]. Furthermore, **local data centres can enable more advanced AI applications** by reducing latency and improving internet traffic, while

[109] See: The local economic impact of a proposed data centre campus in London and Virginia Joint Legislative Audit and Review Commission Report to the Governor and the General Assembly of Virginia on data centers

[110] The study focuses on immediate impacts in terms of investments and jobs and secondary effects on businesses supplying DCs. It does not account for broader spillover effects of DCs on innovation and productivity across sectors or broader economy-wide effects, such as potential impacts on price changes or shifts in consumer behaviour. Available here. The report of the European Data Centre Association projects the European colocation DC sector's GDP contribution to increase from EUR 30 bn in 2023 to EUR 83.8 bn by 2030. Available here. See also: Does GDP growth minus AI capex equal zero?

insufficient domestic compute capacity can create or deepen dependence on external providers. With respect to the impact of AI, recent literature highlights its potential to generate economic benefits, particularly through productivity gains, innovation, scientific discovery and new business models. However, the evidence is strongest for task-level productivity gains and more uncertain at enterprise, sector and macroeconomic level.

Cloud and AI computing services. The second channel of wider effects relates to the **increased adoption of sovereign cloud and AI computing services.** Benefits include enhanced autonomy, improved resilience, reduced dependency, stronger legal and operational control, and better conditions for AI-enabled innovation. Even though several of these effects are hard to monetise, they are economically relevant as cloud and AI computing services increasingly support public administration, healthcare, research, education, justice and law enforcement, cybersecurity and industrial competitiveness. If public authorities depend heavily on a small number of external providers or non-EU jurisdictions, they may face legal, operational, geopolitical and continuity risks. Sovereign cloud and AI services can reduce these risks by providing more diverse supply options, clearer governance, and ensuring stronger alignment with EU and Member State requirements.

A key benefit is therefore **greater resilience and continuity of public services**. Dependence on a limited number of cloud infrastructures can create systemic risks, as disruption in a major provider can affect many services at the same time. The October 2025 AWS outage, for example, disrupted businesses and digital services globally, highlighting this vulnerability[clxxiii]. The World Economic Forum estimated that the 2024 global CrowdStrike outage caused around USD 5 billion in losses, disrupted airlines, banks, healthcare providers, retail payment systems and ATMs worldwide, underlining these system-wide economic consequences[clxxiv]. These examples do not imply that sovereign providers are immune from disruption. Rather, they show the economic relevance of resilience, provider diversity, and reduced single-provider dependency. Indeed, sovereign cloud services **strengthen operational control.** Sovereignty does not only mean storing data in the EU. It also concerns who operates the service, who can access systems, which jurisdiction applies, and whether public authorities retain effective control over sensitive workloads. These are particularly relevant for strategic public sector use cases, such as hospitals, emergency services, tax systems, justice systems or critical infrastructure, where continuity and trust outweigh marginal cost optimisation. In addition, greater availability of credible EU alternatives may have competition and cost benefits. Moving part of its services to EU providers would give public administration the capacity to **improve their negotiating power** and contribute to decreasing this market concentration.

Another relevant potential wider economic effect concerns the **domestic value added through import substitution.** A higher market share for EU providers would shift part of existing and future cloud and AI spending towards services produced within the Union. This would increase the share of wages, profits, reinvestment and tax revenues retained in the EU rather than accruing them abroad. This, in turn, could stimulate additional investment in cloud and AI infrastructure within the EU, enabling European providers to scale up their offerings and strengthen their competitiveness. An illustrative calculation shows the possible order of magnitude.

Considering that the EU-27 public cloud revenues could reach around EUR 320 bn by 2030[111], that the public sector represents around **14%** of demand, and that level 3 and 4 sovereignty levels correspond to 10% of these needs (see description of policy measure 21 here above), this means a

[111] Public Cloud - EU-27 | Statista Market Forecast

market of EUR 320 bn * 14% * 10% = EUR 4.48 bn only addressable by EU controlled providers by 2030[112].

On top of this, it is likely that the signalling effect of European providers being selected for highly sensitive applications will give them increased opportunities in the market, and it can therefore be expected that European providers would increase their market shares also for lower sovereignty levels. Similarly, in the private sector, as regards sensitive sectors subject to a new obligation to pay attention to sovereignty issues, it can be expected that a number of entities will consider giving new business to European entities, which will have less difficulty in demonstrating their sovereignty levels. Sovereign cloud and AI adoption may support productivity gains, although these are still uncertain. McKinsey estimates that Europe could unlock up to **EUR 480 billion annually by 2030** in a "European digital sovereignty" scenario, where AI adoption is high and European providers capture most of the value. In a high adoption but externally dependent scenario, the estimated impact is lower, at around **EUR 375 billion**. In lower-adoption scenarios, the estimated impact falls to around **EUR 80 to 100 billion**[clxxv].

Increased availability of sovereign cloud and AI services may also increase trust among public authorities and thereby **support greater cloudification as a side effect of the intervention**. While for public administrations, the costs of porting or migration are one-off, several benefits may accumulate over time. These include a reduced need to own and manage infrastructure, greater scalability, faster deployment of new functionalities, more flexible cost structures, improved service quality and easier access to advanced analytics and AI tools. Cloud migration is often part of a broader modernisation effort: once the project is completed, the public authority may be freed from managing some underlying IT infrastructure and may be able to add new functionalities more easily. Some literature and case-study evidence point to **total cost of ownership savings in the range of 20–50% for cloudification projects**, although these estimates remain highly context-specific[clxxvi].

At the same time, these benefits must be balanced against the potential price premium (mark-up) of sovereign services. Any additional costs linked to providing sovereign services - compliance costs linked to audits, EUCS certification costs, the use of EU-based infrastructure, higher labour costs for EU-based staff - would be passed on to customers through higher prices.

6.2. Social impact

Employment. DCs are highly automated facilities, and the effect on employment is greater during their construction phase than their operational phases. As reported by stakeholders, construction is typically undertaken by large multi-national construction companies with participation of local teams for the initial phases and non-local specialised teams for fit-out phases. For a 100 MW site, around 1 500 – 2 000 construction employees would typically be on site per day. During the operational phase, approximately 6-8 full time jobs are created for every 1 MW of capacity, with economies of scale appearing as DCs measure beyond 50 MW. Some interviewees also highlighted that they provide offices for some of their larger customers, converting DCs into co-working hubs. When it comes to providing cloud and AI computing services, the EU's shortage in ICT skills can hamper the development of cloud and AI ecosystems, with a limited availability of experts creating a significant gap in an already limited specialist workforce. For AI, only a small proportion of specialists are actively involved in the industry[clxxvii], with many remaining in academia. This results in a low transferability of results to the market and, where transfer is

[112] In lower market growth (250bn) and lower share by the public sector (10%), this would reach EUR 250 bn * 10% * 10% = EUR 2.5 bn by 2030. In higher market growth (390bn) and higher share by the public sector (16%), this would reach EUR 390 bn * 16% * 10% = EUR 6.24 bn by 2030.

successful, companies lack the means to scale up or retain talent. Beyond these direct impacts, cloud and AI computing services play an important role in the digitalisation of other sectors, which has a complex effect on employment[clxxviii]. With respect to the contribution of technological sovereignty, 71% of citizens from the three biggest Member States believe that sovereignty can help create and protect local jobs[clxxix].

Citizens. With regards to DCs, there are documented instances of public resistance against their construction due to environmental concerns, e.g. energy consumption and water security and potential consequences on related prices[clxxx]. However, citizens increasingly use digital services in their daily lives[clxxxi], where cloud and AI computing services and their underlying infrastructure play a vital enabling role. AI, while nascent, is already pervasive[clxxxii]. Citizens stand to benefit from accelerated deployment of nearby compute capacity for low-latency applications like automated driving, decentralised energy grids or assisted surgeries or living. These growing social benefits should help increase the long-term public acceptance of the facilities that power these technologies. Concerning sovereign cloud and AI computing services, a strong majority of citizens from the three biggest Member States support greater sovereignty even if this increases costs and argue that governments should lead the investment and development to achieve this objective. The support drops, however, should this result into a lower spending on public services[clxxxiii].

Some POs have particular social impacts. Under **PO1-A**, the public guidelines and the yearly forum with the involvement of local municipalities, would help increase community trust and engagement. Under **PO1-B**, the social acceptance of DCs is expected to be the greatest, as decisions on DC build-out give a greater role to local authorities and are thus taken closer to citizens. Acceptance can be expected to be particularly high when DCs demonstrably contribute to local communities, for example through waste heat reused in local energy systems. Social acceptance should also be a core attention point of the coordination hub which would disseminate best practices on deployment. Conversely, **PO1-C** is expected to have a detrimental social impact as EU-level decision making on DC deployment is perceived as further away from the citizen. PM18, which belongs to **PO2-B** and is then picked up in **PO2-C**, would have direct social impacts since it focusses on the development of ICT skills where Europe is lagging, resulting in higher employability of citizens. For PO1-A/B/C, the possible effects on consumer electricity prices have not been considered as this would require too many unverifiable assumptions (see next section).

6.3. Environmental impact

DCs in the EU currently are projected to consume around 99 TWh of electricity in 2025, equivalent to roughly 3 % of total EU power generation. Over the next decade, rising capacity will be the primary driver of increased electricity use, though its effect will differ depending on the pace of expansion and the success of energy-efficiency. Electricity consumption and its associated CO_2 emissions represent the dominant environmental impact of DCs and are therefore used as a key proxy for quantifying the environmental impact of additional data centre capacity. Beyond electricity consumption and associated CO_2 emissions, data centres generate environmental impacts across several additional dimensions. Water consumption, embodied emissions in equipment and buildings, refrigerant leakage, and local environmental externalities are also relevant measures of environmental impact[113].

The European Climate Law (ECL) consistency check was performed by comparing the projected electricity use and associated CO_{2e} emissions under each policy scenario with the EU's declining

[113] These impacts could not be systematically quantified at EU level due to lack of harmonised data. Looking ahead and considering the share of the emissions generated for DC construction materials (concrete, steel as well as other materials as semiconductors), the life cycle carbon footprint approach should be another relevant method to measure the environmental impact of each DC project.

grid-emission trajectory toward a 55% GHG emissions reduction target by 2030 and climate-neutrality by 2050. The first subsection presents the quantification of environmental impact in terms of increased energy consumption and CO_2 emissions under the different policy options, with considerations on the interaction between data centre deployment and impacts on the electricity system. Implications of increased data centre capacity on water consumption are then discussed in section 6.3.2.

6.3.1. Impact on electricity use and CO_2 emissions

Under the baseline scenario, total capacity is expected to expand to 46.3 GW[114] in 2036 with an expected modest PUE improvement from 1.29 down to 1.23[115]. Annual electricity use is expected to rise from 99 TWh in 2025 to around 314 TWh in 2036, i.e. an average increase of 11% per year. The cumulative electricity demand over 2025–2036 would amount to 2 571 TWh. Assuming an evolution in the EU grid carbon intensity from 0.25 kg CO_2e/kWh today to 0.16 kg CO_2e/kWh in 2036[clxxxiv], this would correspond to 50 Mt CO_2e in 2036. The environmental impact of PO1-A/B/C is assessed against the increase in electricity demand (in TWh) and CO_2 emissions resulting from additional DC deployment under the different scenarios[116].

Table 10. EU-27 data centre capacity in 2036: electricity and CO_2 impacts vs baseline

Scenario	*2036 Capacity (GW)*	*PUE 2036*	*Electricity Use 2036 (TWh)*	*Cumulative 2025–2036 (TWh)*	*CO_2e /GW 2036 (Mt/GW)*	*Cumulative CO_2e 2025–2036 (Mt)*
Baseline	46.3	1.23	314	2 571	1.18	495
PO1-A	52.2	1.18	339	2 701	1.13	518
PO1-B	65.9	1.12	408	3 028	1.09	576
PO1-C	58.7	1.05	340	2 737	1.01	525

In **PO1-A,** the guidelines would encourage early integration of resource-efficient features, the adoption of renewables and best practices in energy management, while the coordination forum would facilitate dialogue with energy providers. These measures are expected to improve the PUE of new DCs by around 4% by 2036 compared to the baseline, reaching 1.18. Total installed capacity would increase to 52.2 GW and electricity demand would reach 339 TWh in 2036, or about 8% higher than the baseline and cumulative consumption over 2025-2036 would total 2 701 TWh, or 130 TWh more than the baseline. Increased expansion of capacity under this option would push up cumulative carbon emissions by 23 Mt with respect to the baseline. In **PO1-B**, owing to fast-track area identification, Member States would have a stronger hand at linking DC development to sustainable energy availability and avoiding environmentally sensitive sites. EU-level discussions with national authorities are also expected to favour a fast uptake across Member States of sustainability best practices in DC build-out. Altogether, this policy option is expected to deliver an improvement in PUE of 9% by 2036. In this scenario, DC capacity is expected to increase fastest, reaching 65.9 GW by 2036, while annual electricity use would reach 408 TWh by 2036, the highest among all scenarios. Cumulative 2025–2036 demand would exceed 3 000 TWh, approximately 30% above the baseline. Even with continuous efficiency gains, the speed of expansion would push up total energy and resource requirements. Cumulative CO_2 emissions are expected to be 82 Mt higher than the baseline over the decade. However, average CO_2e emissions/GW decline 12% faster than in the baseline scenario due to the expected improvements in PUE. With **PO1-C,** EU R&D funding (PM8) is expected to support the development and

[114] Data centre capacity includes private sector, i.e. colocation and hyperscalers, and public sector capacity.
[115] For additional information concerning expected PUE changed under the different Policy Options, please see Annex 4, Section 2.3.5.
[116] The baseline assumes that electrical grid limitations remain an issue in certain primary markets such as Ireland and the Netherlands. However, it considers that regulators and operators in several markets have begun investing in grid modernisation and demand management.

gradual uptake of sustainable innovations, especially after an initial phase of testing and demonstration. These may include AI-driven energy management, advanced cooling systems, solutions for waste heat reuse and renewable and storage integration. Strategic funding for deployment (PM9) would also be used to incentivise projects incorporating highly sustainable features, making eligibility conditional on sustainability criteria. These two measures focusing on targeted grants or technical support will be designed to stimulate the development, testing and market uptake of advanced solutions with the objective of considerably reducing PUE and WUE levels over a 10-year horizon. This type of intervention could help smaller colocation providers reduce PUE as they would aim to facilitate upfront R&D investments, pilots and CAPEX into innovative technologies that small operators struggle to finance compared to hyperscalers[clxxxv]. EU-level identification of fast-track areas (PM10) would ensure that facilities are deployed where they are least environmentally damaging at continent level. Capacity under this option is expected to reach 58.7 GW by 2036, with the strongest efficiency gains: PUE falls to 1.05 (–15% with respect to the baseline). Despite 27% higher capacity than the baseline, total electricity use remains close to PO1-A at 340 TWh, so is the cumulative consumption over 2025–2036. Due to cleaner electricity sourcing, stronger PUE reductions and general forecasted decarbonisation of the grid mix, average CO_{2e} emissions/GW are expected to decline 21% faster than in the baseline scenario[117]. Across all scenarios, electricity use at least triples between 2025 and 2036. However, with policy measures under PO1-C, stronger efficiency standards and renewable integration are expected to contain DC power demand to around 13% of EU electricity generation.

Finally, under **PO2-B** and **PO2-C**, the cross-border re-use of cloud and AI capacity among Member States through the federation would be inducive of environmental savings: a rough estimation points to 5% energy efficiency improvement for 10% increase in server utilisation rate[clxxxvi].

The resulting emissions would increase across all scenarios due to growing DC electricity demand. However, CO_{2e} emissions per GW of added capacity would decline much faster under PO1-C than under the baseline, owing to the stronger reduction in PUE and gradual adoption of sustainable energy integration measures. The baseline pathway is not compatible with long-term climate neutrality goals, as it leads to increased energy demand without integrating sustainability requirements. Policy intervention is essential to uphold consistency with the ECL and ensure that possible national DC acceleration policies do not result in a race-to-the-bottom in terms of sustainability and minimise environmental impacts and grid strain[clxxxvii].

As mentioned under section 2.2.2., grid capacity limitations are also real and increasing barriers for the development of data centre capacity. The International Energy Agency highlighted that waiting times for grid connection in key data centre hubs range from two to ten years due to capacity limits and congestion, thus slowing down project development and diverting investment to regions with available grid capacity[clxxxviii]. In this context, it is important to note the positive contribution which DCs – if properly leveraged – can make to grid stability, notably by offering flexibility services[118]. The co-location of energy generation on a DC site can help reduce grid stress and DC investments have the potential to also boost investments in grid infrastructure.

6.3.2. Impact on water consumption

Data centres are also becoming a significant and rapidly growing source of **water consumption**, with implications for regional water security and climate resilience. Depending on the cooling

[117] Carbon footprint is mostly driven by scope 2 energy consumption. To reduce climate impact, low-carbon energy use should be incentivised.
[118] Notably, due to their storage capabilities, data centres present a unique opportunity to enhance power system flexibility. See for example: Data centres as a source of flexibility for power systems - ScienceDirect.

technology used, their cooling systems can require large volumes of freshwater, often millions of litres per day for hyperscale facilities, placing pressure on local supplies, especially in drought-prone or water-stressed areas. As demand for cloud services and AI model training accelerates, water use is expected to rise unless mitigated through efficiency measures, site-specific resource planning, and low-water or water-free cooling technologies. Estimates suggest that data centres across the EU consumed around 76 bn litres of water in 2025. At global level, the International Energy Agency estimates that water consumption by data centres amounts to approximately 560 bn litres per year[clxxxix], implying that the EU-27 accounts for around 14% of global data centre water consumption. When assessed against broader metrics related to water use, data centres represent a relatively small share of overall water pressure. Total freshwater abstraction in the EU has decreased by 19% between 2000 and 2022, corresponding to a compound annual growth rate of -0.8%, according to the European Environment Agency[cxc]. Extrapolating this rate to 2025 suggests that, out of an estimated 192,000 million m³ of freshwater abstracted annually in the EU-27, data centres accounted for 0.04%, i.e. remaining well below the levels observed in international counterparts. As data centre capacity is expected to grow in the next years, overall water consumption by data centres is also foreseen to increase. However, this trend could be alleviated by an industry shift towards more sustainable and resource-efficient operations. The adoption of advanced cooling technologies and improved practices is expected to consistently reduce water intensity over time. A reduction in Water Usage Effectiveness (WUE) from current levels of 1.8 to 0.6 litres per kWh over the next decade, in line with the Climate Neutral Data Centre Pact's target of WUE levels below 0.4 litres per kWh by 2040, and ongoing efficiency improvements by hyperscalers, could substantially limit water demand. Under these assumptions, water consumption growth could be reduced by around 8 percentage points in CAGR, resulting in total water consumption that is approximately half of what would be observed in the absence of comparable efficiency oriented measures.

Against the sector's continued growth, measures that incentivise resource-efficient investments, technological improvements and a balanced distribution of new data centre capacity across Member States, with particular attention to water-stressed regions, are key to reduce the environmental impact also in terms of water consumption. As noted above, overseeing the water use of data centres is crucial not only for environmental sustainability but also for social equity and economic stability. Given the local nature of water systems, the increase in data centre capacity can impact water supply reliability and influence drought resilience in specific areas. The analysis highlights the need for governance mechanisms that ensure new infrastructure aligns with sustainable water management, transparent reporting, and equitable access to shared water resources.

6.3.3. Other key metrics concerning environmental footprint

Research has shown that focusing uniquely on electricity, CO_2 and water usage overlooks key environmental impact categories linked to building new data centre capacity, in particular as grids are expected to become more sustainable in the future. Studies have highlighted the importance of embodied impacts, i.e. environmental impacts associated with construction materials, mechanical and electrical equipment and IT hardware maintenance, which can become a relevant portion of the overall data centre footprint over time[cxci]. A recent peer-reviewed paper similarly highlights the need for comprehensive life cycle assessments of cloud infrastructure to measure environmental impact[cxcii]. Several equipment and IT hardware pieces needed in data centres, especially if in constant use, may need replacing upon reaching end-of-life. The proper collection and treatment of these waste electrical and electronic equipment (WEEE) from data centres is

necessary to protect human health and the environment, in particular as regards depollution and hazardous substances, as well as the recovery of materials from recycling[119].

Another environmental factor in DC development remains sustainable cooling. While powering the cooling is an integral part of overall energy consumption, using low global warming (GWP) potential refrigerants remains important. Refrigerants used in cooling systems can pose significant climate challenges due to leaks of high-global warming potential fluorinated gases (F-gases). The European Environment Agency outlines why fluorinated greenhouse gases are a key focus for mitigation and tracks EU actions in this area[120]. Moreover, at EU level, the recast F-gas regulation combined with the ICT Taxonomy provide guidance on the types of sustainable refrigerants to be used for cooling EU DCs[121].

Lastly, environmental assessments and Scope-3 frameworks[cxciii] bring attention to other impactful areas, e.g. supply-chain emissions and waste from equipment and infrastructure (Scope 3), emphasising the need to consider other parameters beyond electricity usage for accurately monitoring the environmental footprint of data centres in the future.

7. HOW DO THE OPTIONS COMPARE?

This chapter evaluates the policy options in terms of their effectiveness, efficiency, coherence, subsidiarity and proportionality. It brings together the results of the preceding impact analysis to examine how each option performs against these criteria and highlight their relative strengths and weaknesses. It then presents the results of the sensitivity analysis conducted, using best- and worst-case scenarios to derive confidence intervals for testing the robustness of the cost-benefit results under varying assumptions. The final section then focuses on the comparison of the options, presenting their overall performance across the different criteria.

7.1. Effectiveness

The analysis of effectiveness examines the extent to which the policy options under consideration are expected to contribute to the achievement of the general and specific objectives of this initiative. As outlined in section 5.2., the first set of options primarily addresses SO1 and SO2, while the second set has been designed to better address SO3 and SO4. The table below illustrates the relationship between the policy objectives and the assessment criteria, which served as initial benchmarks for evaluating the potential effectiveness of the options.

The assessment draws primarily on evidence gathered through literature review and desk research, complemented by interviews, the CATI survey, and validation workshops. While this section presents the analysis mostly in qualitative terms, the same evidence base, including survey results, was integrated into a multi-criteria decision analysis (see Annex 4, section 6) to evaluate the effectiveness of the proposed measures, alongside other assessment criteria.

Table 11. Links between objectives and assessment criteria

General objective	Specific objectives	Assessment criteria
Ensure the functioning of the internal market	**SO1** – Increase computing capacity in the EU through innovative and sustainable	• Expected increase in EU installed computing capacity (MW) • Expected improved PUE of new data centres

[119] As announced in the Clean Industrial Deal (CID) Communication adopted 26.02.2025, the Commission is preparing a review of the WEEE Directive as a pillar of the upcoming Circular Economy Act (CEA) proposal intended for later in 2026, in particular with a view to improve areas identified in the Evaluation of the WEEE Directive published 02.07.2025, including WEEE collection, treatment of WEEE, and recovery of critical raw materials (CRMs) embedded in various WEEE.

[120] See: EU progress under the hydrofluorocarbon phase out set out in the EU F-gas Regulation | Hydrofluorocarbon phase out in Europe | European Environment Agency (EEA)

[121] See Regulation (EU) 2024/573: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32024R0573

General objective	Specific objectives	Assessment criteria
for cloud and AI computing services and secure the conditions necessary for the competitiveness of the Union's industry and the resilience of its public sector as users of such services	technologies	• Increase in the number of pilots launched and innovative technologies, e.g. immersion cooling for energy efficiency, adopted in new data centre projects.
	SO2 – Ensure attractive conditions for the deployment of sustainable and innovative computing capacity	• Expected reduction in the time needed for data centre permitting and total administrative proceedings. • Expected reduction in underutilised land (share of identified viable sites used). • Share of new capacity deployed outside existing hubs/underserved areas. • Additional investment in data centre capacity driven by better investment conditions for data centre projects.
	SO3 – Decrease the overall reliance on non-European cloud and AI computing services	• Expected increase in the market share of European cloud and AI computing service providers serving highly critical use cases • Expected reduction in dependency concentration on non-EU providers
	SO4 – Enhance the resilience of supply of cloud and AI computing services, in particular in the public sector	• Expected increase in the number of public sector contracts supplied by providers meeting the sovereign services at level 2, 3 or 4 scored under level 2, level 3 or 4 • Expected increase in the (re-)use and sharing of open source solutions • Expected increase of federated resources across the public sector and use of the joint procurement of cloud and AI services

Regarding **SO1** (**increase computing capacity in the EU through innovative and sustainable technologies**), **PO1-A** would provide a limited effect. An expanded working group and structured forum are expected to reduce coordination and information frictions mainly linked to inconsistent permitting and zoning procedures across Member States. The guidelines focused on sustainability would be designed to translate "innovative and sustainable" technologies into best practices for data centres. These would aim to complement the existing reporting obligations under the EED with concrete instruments to improve compliance with sustainability requirements and allow an earlier integration of efficiency-related considerations in project design. At the same time, being voluntary instruments based on ad hoc participation or adoption by businesses, these measures are expected to indirectly and slightly increase computing capacity in the EU and reduce PUE with respect to the status quo scenario. While the option is expected to improve the quality of new capacity, its concrete contribution to additional MW or innovative technologies for energy-efficiency is expected to be moderate. **PO1-B** is expected to be more effective at increasing EU-based computing capacity, with the strongest direct impact on additional data centre deployment. This is expected as the result of more favourable growth conditions, driven by simplification measures, faster permitting and potential public support by Member States. The national facilitator (PM4) and nationally defined strategies, including fast-track areas (PM5) are expected to reduce permitting timelines and time needed for data centres to connect to the grid, while ensuring that projects also locate where grid capacity, land and water constraints make sustainable expansion of capacity technically feasible. This would foster lower PUE levels across the EU as access to the zones would also be linked to sustainability performance. Without this linkage, adverse consequences linked to excess grid stress or carbon-intensive expansion would undermine SO1. The regular monitoring of compute capacity and national strategies would ensure that the intervention is effective in closing the demand-supply gap, without under or over supplying capacity across the EU. **PO1-C** is expected to be less effective than PO1-B, due to the addition of

a decision step at EU-level over what is currently decided at national or regional level. PM10 consolidates the 27 national permitting and fast-tracking systems for data centre deployment into a single EU-level decision framework. This centralisation is expected to create different types of inefficiencies for data centre deployment. The first one would be related to the number of projects that would be processed in parallel. While under PO1-B access to fast-track areas can be authorised in parallel across MS, under PO1-C projects must pass through a common EU-level decision layer, which is likely to limit the throughput of projects that can be supported. The lower effectiveness of this option was also strongly raised by stakeholders during workshops and interviews, where several operators and public authorities expressed their concerns that an EU-coordinated process would slow down procedures rather than accelerate deployment. They specifically mentioned that top-level identification of fast-track areas for projects would be less able to reflect geographical and local specificities, e.g. related to grid conditions or community impacts. While under PO1-B, the social acceptance of DCs is expected to be the greatest, as decisions on build-out would give a greater role to local authorities and are thus taken closer to citizens, EU-level decision making on DC deployment will likely be perceived as taken far away from citizens. This option is expected to be mostly effective in promoting sustainable technologies through EU R&D funding (PM8) and EU deployment funding (PM9). These measures are expected to improve technology readiness, e.g. in advanced cooling or energy management, while also de-risking first-of-a-kind projects of a strategic interest. Therefore, this option is expected to perform better than the other options and the baseline on long-term sustainable computing capacity, while below them in terms of short to medium-term delivery of additional data centres.

All POs dealing with the dependence on cloud and AI computing services provided by non-EU providers (**PO2-A, PO2-B and PO2-C**) are expected to have an indirect impact on DC capacity in the EU, particularly **PO2-C** as one of the criteria to identify sovereign services across all levels includes the need for infrastructure to be located in the EU. Therefore, if the demand for sovereign services increases, the infrastructure in the EU will also have to increase.

Looking at **SO2** (**ensure attractive conditions for the deployment of sustainable and innovative computing capacity**), **PO1-A** would provide a relatively low-cost way to address the bottlenecks that affect DC build-out in the EU. However, it is expected to have a limited effect on addressing permitting delays, access to resources and capital for strategic projects. Under this scenario, attractive conditions for data centre deployment are built through structured dialogue and guidelines, which contribute to reduce uncertainty for businesses and investors during site selection and project design. The reduced transaction costs allow operators to face fewer project redesigns, while authorities also rely on shared benchmarks. This is expected to somehow reduce permitting timelines by a few weeks and lower regulatory risks but would not consistently change the economics of new data centre projects. Similarly, this option is expected to lead to improvements in established markets, without unlocking significant capacity deployment in other regions or alternative locations, other than through natural market dynamics. **PO1-B** shows a significant potential to reduce bottlenecks for DC buildout, thus ensuring more attractive investment conditions. The introduction of fast-track areas would address inefficient procedures, uncertainty in approval processes and delays that operators cite as critical barriers. The systematic mapping of suitable sites and removal of zoning uncertainty are expected to make land investment-ready and reduce underutilised yet suitable sites. In parallel, the creation of a project facilitator aims to accelerate administrative processes and is expected to decrease the time for

building a new DC facility by at least 6 months[122]. This improved timeline reliability is translated as higher project Net Present Value and Internal Rates of Return (IRR) for investors, with an expected increase in private capital mobilisation. Under this option, projects' IRR would rise by over 80 basis points with respect to the baseline, increasing from 9.86% to 10.70%. This shift is expected to enhance investor appetite, as confirmed by interviews with investors, who highlighted that this shift in IRR can reposition assets within investor target bands, improving competitiveness against alternative infrastructure investments and affecting bankability[123]. This is particularly relevant for mid-sized European data centres (typically 5–25 MW), which are aligned with institutional investment ticket sizes but face tighter margins and higher relative development risk than hyperscaler projects. Where needed, national funding support (PM6) can help lower capital and operating costs, improving project bankability and investment decisions, especially for smaller providers, thus lowering their entry barriers in the market. Sweden has provided a useful example of how tax incentives could be poorly managed if not linked to specific energy objectives and subsequent evaluation[cxciv]. Monitoring deployment is also expected to increase policy credibility and transparent information for investors. By targeting the drivers of geographic clustering (i.e. divergent frameworks, path dependency, uninternalized externalities) and lowering entry barriers in underutilised regions, this option is expected to unlock investment in secondary markets, e.g. Italy or Portugal, and in developing regions, e.g. Bulgaria[124], leading to a rebalancing of capacity across the EU. **PO1-C,** although effective at addressing fragmentation and promoting harmonisation through EU-level coordination, is expected to be less effective in achieving relevant reductions in permitting duration and financing conditions of projects. On one hand, R&D funding and deployment funding would be a relevant political signal towards the development of sustainable digital infrastructure. EU-level coordination would also help minimise regulatory hurdles for cross-border investors. With respect to promoting a more geographically balanced distribution of capacity and increase land optimisation, EU-level decision making is, in principle, best placed to steer deployment towards an optimal territorial allocation of computing infrastructure. However, its effectiveness in reaching this objective is contingent on local engagement, which may be harder to secure than under PO1-B. Industry consultations highlighted that the creation of additional governance layers could slow down decision-making processes, especially if still requiring national or local review. Thus, this option is expected to be less effective than PO1-B in addressing barriers to deployment.

For **SO3** (**decrease the overall reliance on non-European cloud and AI computing services**)**, PO2-A** is expected to have limited effectiveness relative to the baseline. Harmonised criteria, guidelines and a dedicated conference, are expected to increase clarity and promote a more coherent understanding of the concept of sovereignty. This may reduce information asymmetries and improve comparability of service offerings, especially in public procurement. However, these measures are unlikely, on their own, to shift demand away from non-European cloud and AI computing services. In the absence of clear and robust assessment mechanisms to verify the

[122] This has been confirmed through interviews with stakeholders and validated during a final workshop in the context of the supporting study. The impact has been assessed on the basis of an overall 18-month permitting period for data centre deployment. However, any reduction in this timeline, including for example through the introduction of as 12-month deadline would further increase Europe's attractiveness as a location for data centre investment

[123] Interviews with investors confirmed that data centre investments are evaluated across a wide risk-return spectrum, broadly consistent with market benchmarks positioning core infrastructure targeting around 7-9% IRR and core-plus assets around 10-13%. Expected returns depend strongly on asset maturity and risk profile: stabilised, fully built platforms with secured power and long-term contracts are treated as lower-risk assets, while development-stage projects face higher execution risk related to permitting, power availability, equipment procurement, and commercialisation. Equity investors typically target "single digit returns plus a risk premium," with materially higher expectations for projects exposed to development, energy, or commercial risk.

[124] During stakeholder interviews, and as mentioned above, Bulgaria was identified as lacking a clear classification of data centres in its permitting system, creating long delays and deterring investment in the country.

harmonised criteria, sovereignty claims would remain self-declared and the notion of sovereignty risks remaining a marketing tool with little or no effect in trust building. Ensuring the effectiveness of the interoperability provisions of the Data Act would contribute to creating opportunities for EU providers to build integrated offers. However, the Data Act's effects remain to be seen, given its recent adoption. The main consequences of this option would reside in the gradual standardisation of the services, coupled with measures to promote interoperability, rather than a structural change in procurement or deployment choices, which would alter existing market dynamics. **PO2-B** is expected to be moderately effective in meeting this objective. A voluntary sovereignty framework combined with voluntary award criteria that give weights to factors such as the resilience of the EU cloud supply chain are expected to strengthen trust in cloud and AI computing technologies, especially for the public sector. Through spillovers, parts of the private sector could also be impacted, notably in sectors where sovereignty considerations are strategically important. By enabling the federation of computing capacity, as opposed to procuring from external providers, the option would produce more concrete substitution effects than PO2-A or the baseline. The option is expected to broaden the range of eligible procurement models for public authorities, e.g. in terms of tender design, vendor evaluation, without mandating a universal switch to sovereign solutions. The vendor-neutral cloud and AI computing services training programme is also expected to reduce the reliance on few, vendor-specific training and certification programmes. The overall effectiveness of the option in decreasing the reliance on non-European cloud and AI computing services would depend on authorities' administrative capacity, procurement design and consequent market responsiveness. It could reduce some exposure to third country dependencies if contracting authorities choose services with stronger EU control features. This PO's weakness lies in the voluntary nature of the proposed measures, which could result in uneven adoption across Member States. **PO2-C** is expected to be the most effective option in reducing the reliance on non-EU cloud and AI services. The combination of joint procurement mechanism, the mandatory sovereignty risk assessment and mandatory award criteria, along with the promotion of open source solutions is expected to have more substantial impact on market outcomes compared to other options and the baseline. Unlike softer or voluntary measures, this package embeds an approach to sovereignty into market access and purchasing decisions, going beyond mere clarification or incentives. First, the **mandatory sovereignty risk assessment** for procuring cloud and AI services plays a crucial role in embedding sovereignty and dependency-related considerations into procurement decisions. This measure ensures that contracting authorities procure services considering the sovereignty implications of decisions, leading to more informed choices. By bringing clarity with respect to the use cases for which cloud and AI computing services shall be procured under specific sovereign levels, the approach contributes to reducing the reliance on non-EU cloud and AI services. In fact, levels 3-4, which are estimated to cover 10% of the public sector's needs, would need to be served by EU providers to address and ensure the protection of public order in the public sector. Most procurement cases would fall under intermediate levels of sovereignty, where non-EU providers can participate. However, EU providers are likely to face fewer difficulties in complying with the sovereignty requirements, giving them a competitive edge (the reasoning for these numbers is presented under the descriptions of policy measures PM15 and PM21 in section 5.2.2, and the coverage of the necessary range of services by EU providers in section 2.3.1). Moreover, with a view to reducing critical dependencies, the **non-price award criteria** would allow public authorities to procure cloud and AI computing services with a higher level of local added value. The overall monitoring framework managed by the Commission would support Member States in assessing the market presence of EU providers. By advancing an EU-coordinated procurement and support framework for sovereign services, the option is also expected to increase trust in cloud and AI computing

services and accelerate the cloudification of on-premises solutions of the most critical use cases, while creating market opportunities for sovereign European cloud providers. This approach is also expected to create broader spillover effects beyond the public sector. Notably, the mandatory nature of the sovereignty framework as well as the proposed extended risk assessment for essential entities of the private sector listed under Annex I NIS 2 to address sovereignty-related risks are expected to create a wider spillover effect compared to that of PO2-B. The main challenge that could hinder the adoption of sovereign services in the private sector could be a "sovereignty-premium price" whose range remains subject to be established (see discussion under section 2.3.4). However, several companies in critical sectors have already publicly manifested their interest in those solutions and are moving towards that direction[125]. This would be amplified through the SME support scheme fostering cloud and AI adoption among SMEs, and the creation of toolbox for the integration of EU providers solutions, which is expected to increase the visibility of EU sovereign services. Building on this, the **joint procurement mechanism** allows public sector organisations to pool their purchasing power, creating a larger and more stable market for *inter alia* EU providers. This mechanism is also expected to attract more investment, reduce costs and improve the overall competitiveness of EU providers, making them comparable alternatives to non-EU providers[126]. Moreover, the promotion of open source solutions within public administrations would further reinforce this objective by improving fairness and transparency, reducing vendor lock-in, stimulating competition among providers, and opening the market to alternative solutions and to new entrants. This measure encourages innovation and local development, creating opportunities for European companies to thrive in the cloud and AI market, and contributing to the growth of the open source services sector in Europe. Overall, the measures included in policy option PO2-C work together to reduce the reliance on non-EU cloud and AI services, promote European sovereignty, and foster a robust and competitive European cloud and AI ecosystem. By addressing the risks associated with dependency on non-EU providers with a granular, layered sovereignty framework and promoting the development of European solutions, this option is expected to have a lasting impact on the market, creating a more sustainable and resilient foundation for the public sector's digital transformation.

For **SO4 (enhance the resilience of supply of cloud and AI computing services, in particular in the public sector), PO2-A** is expected to have a very limited effect due to the soft nature of the measures. While common criteria and guidance may improve awareness of relevant risks and encourage the use of more coherent definitions by public authorities, they would not materially increase switching capacity, supply redundancy or operational continuity in the event of disruption. The option thus addresses only part of the information problem but not the structural sources of fragility and trust. This would result in having a marginal effect on reducing exposure to service disruption, or non-EU dependencies, especially in the public sector. **PO2-B** is expected to be moderately effective in improving the resilience of supply of cloud and AI computing services. The federation would contribute to ensuring that specific use cases are served by services with increased EU control. Federation is especially relevant from a resilience perspective as it supports the diversification of dependencies, and reduces the risks associated with reliance on a single external provider. The training programme on vendor–agnostic technologies and voluntary award criteria are also expected to expand the market for resilient and locally managed cloud and AI computing services. Nonetheless, as mentioned above, the voluntary implementation of these measures could limit their consistent implementation across the EU. This would result in uneven

[125] See for instance Airbus who recently announced their activities to migrate their critical workloads to a European cloud provider.
[126] The outcome of the recent DIGIT tender for cloud services is testament to this. Commission advances cloud sovereignty through strategic procurement

resilience gains: authorities with higher procurement maturity would likely benefit more, while others may not implement the framework in a way that changes their risk exposure. **PO2-C** is expected to have the biggest effect on resilience. The establishment of an actionable and comprehensive sovereignty assessment framework provides national authorities with a more robust mechanism to procure and uptake cloud and AI computing services, protecting critical use cases where public order is at stake. The framework allows for the diversification of dependencies, and services from non-European providers would still be able to qualify for 90% of the public sector's needs. The use of harmonised public procurement award criteria would also contribute to the public sector's resilience for specific services since procured services would have a higher EU added value. Moreover, the joint procurement mechanism is expected to simplify the procurement of cloud and AI computing services and allow public authorities – especially the smaller ones – to achieve better commercial and contractual terms. Finally, the promotion of open source technologies would further strengthen resilience by reducing dependencies on proprietary systems. Altogether, these measures would directly reduce exposure to non-EU dependencies and single provider concentration risks, strengthening the resilience and autonomy of cloud and AI services, particularly in the public sector.

With respect to the **general objective of promoting competitiveness while strengthening strategic autonomy**, the options differ in effectiveness and in the balance they strike between the two dimensions. In terms of promoting competitiveness, the first set of options differs in the expected ability to accelerate data centre deployment and reduce investment barriers. **PO1-A** would have a limited but positive effect by improving coordination and sharing good practices, although its voluntary nature means that it may not significantly reduce permitting, infrastructure or investment bottlenecks. **PO1-B** would be the most effective option, as national-level legislative and financial measures could be tailored to local conditions, including designated areas, fast-track procedures, public support for projects and capacity monitoring. This would directly support faster deployment and investment certainty. **PO1-C** could also support competitiveness through EU-level funding and fast-tracking, but may be less responsive to local permitting, energy and land-use constraints. Strategic autonomy would be strengthened under all options to the extent that additional capacity is built in the EU, with the greatest practical effect expected under PO1-B. **PO2-A** is expected to make a modest contribution to competitiveness by reducing information frictions and clarifying some notions, but it is unlikely to improve the competitive position of EU-based providers or to alter the dependency structure of the market. Its contribution to strategic autonomy would therefore also be limited. In practice, it would preserve the status quo in market structure while improving transparency. As a result, it is unlikely to achieve the general objective. **PO2-B** is based on a more comprehensive set of measures that may impact competitiveness and strategic autonomy. Its contribution to competitiveness would come from stronger demand for sovereignty-audited services, greater contestability through federation and interoperability, and reduced lock-in. Its contribution to strategic autonomy would come from lower dependency in sensitive use cases and a gradual expansion of EU-controlled capacity. However, the option may not be strong enough to overcome incumbent scale advantages, so both competitiveness and autonomy gains may remain incomplete. **PO2-C** is likely to deliver the strongest gains in strategic autonomy. It is the option most likely to expand the market position, scale and credibility of sovereignty-qualified providers, and therefore the most likely to change the structure of the market in favour of strategic autonomy. Over time, this could support competitiveness if stronger EU demand fosters scale, innovation capacity, local value creation, and broader ecosystems around interoperable and open solutions. In terms of achieving autonomy, this is the option which most effectively prevents unlawful access to European data through non-European laws that have an extraterritorial reach, but in a proportionate way. In fact, MS can decide which use cases should

fall under higher levels of sovereignty assurance, based on their considerations. To support the Single Market, the Commission would issue EU-level guidance for MS to conduct their risk sovereignty assessments. While not ensuring a unique outcome, this would be a signal for authorities to converge towards a unique approach. Doing this would allow providers to operate more easily across the EU, thanks to common criteria and approaches to which services can be served under different sovereignty levels. Competitiveness is also preserved because the sovereignty framework is devised in a way to better align MS with the available offer from European operators thanks to the market monitoring reports provided by the Commission. These would allow Member States to integrate a market reality check in their risk assessments, avoiding situations such as tendering at Level 3 where competition is limited or no solution exists. These market monitoring reports would also act as a powerful guidance for EU providers to prioritise the development of their offering, thus incentivising the emergence of a competitive European alternative. In terms of long run competitiveness, the use of clear sovereignty levels for different use cases based on a risk sovereignty assessment is also expected to reinforce trust and the uptake of cloud and AI technology across the EU economy and society[127].

The overall effectiveness assessment with respect to each specific objective is presented below using a symbolic scoring, using ranking indicators that go from "o" no relevance to "very effective", with respect to the baseline.

Table 12. Effectiveness of the Policy Options against the Specific Objectives

	SO1: Increased computing capacity through innovative and sustainable technologies	**SO2:** Attractive conditions for the deployment of computing capacity	**SO3:** Reduced reliance on non-EU providers	**SO4:** Enhanced resilience of supply of cloud and AI computing services
Policy option 1A	+	++	o	o
Policy option 1B	+++	+++	o	o
Policy option 1C	++	++	o	o
Policy option 2A	+	o	+	+
Policy option 2B	+	o	++	++
Policy option 2C	++	o	+++	+++

Legend: o no relevance; + limited effectiveness; ++ effective; +++ very effective

7.2. Efficiency

The table below presents a qualitative summary of costs and benefits of the Policy Options borne by the main stakeholder groups analysed under section 6.1., i.e. data centre operators, cloud and AI service providers, essential entities of the private sector, public authorities and the European Commission, mostly calculated using the standard cost model and net present value framework[128]. Given the uncertainty around the estimates, the results are presented using "+" and "-", which reflect indicative ranges rather than precise values. The objective is to present the likely direction and scale of each option compared to the baseline. Positive signs indicate benefits, while negative ones indicate costs, while the number reflects the order of magnitude of the quantified impact. The

[127] This issue was recently illustrated by the postponement of Finland's electoral management system cloudification, previously awarded to AWS, and France's switch from US solutions to open source equivalents to serve public sector video conferencing needs are illustrations of this broad trend.

[128] The table does not include the impact on SMEs, which is discussed only qualitatively in the previous section. Additional information on quantified costs and benefits for SMEs under PM23 can be found in Annex 4 and are reported in the efficiency overview of the preferred package below.

table does not incorporate non-market social and environmental externalities. These effects are discussed in the respective sections 6.2, 6.3 and further below as a relevant part of this impact assessment.

Table 13. Summary of costs and benefits of the policy options – indicative ranges based on central estimates of NPV for 2027-2036 and qualitative estimates, compared to the baseline

	Difference to the Baseline					
	PO1-A	**PO1-B**	**PO1-C**	**PO2-A**	**PO2-B**	**PO2-C**
Data centre operators						
Benefits	+	+++	+++	N/A	N/A	N/A
Costs	–	–	–	N/A	N/A	N/A
Cloud & AI service providers						
Benefits	N/A	N/A	N/A	+	++	++
Costs	N/A	N/A	N/A	–	–	––
Essential entities of the private sector						
Costs	N/A	N/A	N/A	N/A	N/A	––
Public authorities						
Benefits	+	++	+	N/A	++	++++
Costs	–	––	–	–	––	––
European Commission						
Costs	–	–	–	–	––	––
Wider economic effects	+	++++	+++	+	++++	++++
Total benefits	+	+++	+++	+	+++	++++
Total costs	–	––	––	–	––	––
Net benefits	–	+++	+++	–	+++	++++

Legend: N/A not applicable; + small benefit <€100m; ++ moderate benefit €100m-5bn; +++ large benefit €5-20bn; ++++ very large benefit >€20bn; - small cost <€ 100m; -- moderate cost €100m-5bn; --- large cost €5-20bn; ---- very large cost >€20bn

Overall, all the options except for PO-2A and PO1-A are expected to generate positive net benefits relative to the baseline. For these options the expected benefits outweigh the expected costs. PO2-C is expected to generate the highest net benefits among all options. Although it also entails higher quantified costs, these remain lower than the expected benefits. PO1-B, PO1-C and PO2-B also show strong efficiency, with large, expected benefits relative to the expected costs.

7.3. Coherence

In terms of **external coherence**, the proposed POs are consistent with existing initiatives. They seek to close remaining gaps with respect to reaching the objectives. See annex 7 for details.

PO1-A/B/C complement and leverage other initiatives: PO1-A expands the existing Alliance on Industrial Data, Edge and Cloud. PO1-B/C builds on the future Regulation on accelerating and streamlining environmental assessments, which will simplify and speed up environmental screenings and assessments. It allows for sectoral legislation to reference a toolbox with additional favourable provisions for strategic sectors or categories, which CADA will do for DC projects built in acceleration areas[129]. These additional DC-specific support measures are necessary to rapidly close the capacity gap and can only be delivered in a dedicated instrument. Similarly, PO1-B/C uses the rating scheme for DC sustainability under the EED to identify which DCs are sustainable and can benefit from acceleration measures. In the same vein, PO1-B/C complements

[129] PO1B/C takes the creation of a single point of contact for environmental assessments for granted and complements it with a facilitator (PM4) who would accompany the DC operator in this and other administrative stages (environmental assessments but also other permitting requirements related to zoning, land allocation and building).

the Grids package by ensuring DC location considers grid availability, information is exchanged sufficiently in advance to feed into grid planning and hence ensure timely connection of DCs. Finally, none of the PO1s will overlap with the Industrial Accelerator Act which focusses on the industrial manufacturing sector to which DCs do not belong.

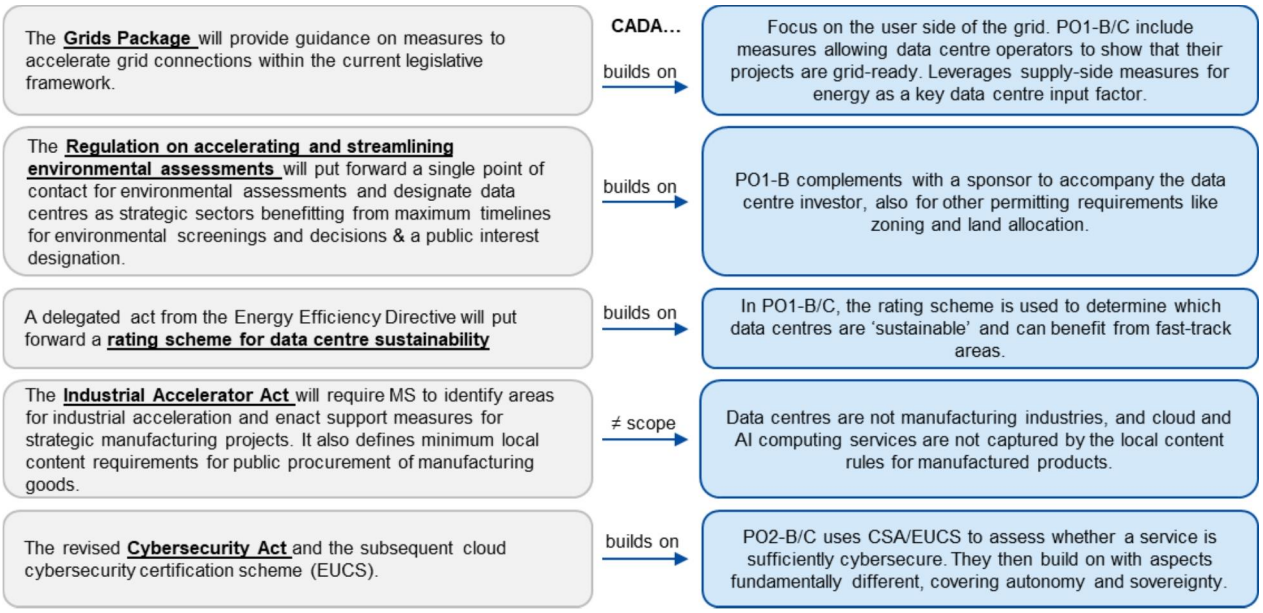
PO2-B/C will complement the Public Procurement Directives 2014/23, 2014/24 and 2014/25 by ensuring that the public procurement of cloud and AI computing services is covered by a specific sectoral approach which caters for its specificities: For example, for reasons of strategic autonomy, it is of utmost importance to ensure that highly critical public sector use cases of cloud and AI computing services rely on services which are shielded from third-country data access and possible interference with service continuity (PO2-B/C). This is different from a blanket 'Buy European' approach, which may be considered as part of the ongoing revision of the Public Procurement Directives. Due to today's strong reliance on non-European CSPs, a blanket 'Buy European' approach would not be suitable for public procurement. Instead, for reasons of public order protection, PO2-B/C put forward ways of mitigating incrementally existing dependencies through award criteria rewarding, for example, the integration hard- or software from outside the countries of dependencies. On the side of contracting authorities, this approach implies that they will have to comply with the horizontal requirements laid down in the Public Procurement Directives as well as the *lex specialis* of CADA, especially under PO2-C. In view of the ongoing review of the Public Procurement Directives, the preparatory work on the impact assessment supporting the formulation of a Public Procurement Act includes a framework regulating the use of 'EU preference' provisions in sectorial legislations. The measures foreseen in the impact assessment supporting the Public Procurement Act would underpin the approach taken in CADA both in terms of tools (award criteria) and justification (demonstrable relation to public order and proportionate approach to risk mitigation). To prepare the grounds for a faster uptake of cloud services by the public sector, CADA will be accompanied by a Recommendation on a single EU-wide cloud and AI policy for public administrations and public procurement translating the Regulation's approach to public procurement into ready-made tender specifications.

While the Data Act opens the path to a possible reduction of dependencies on non-EU providers by enabling switching, it does not directly incentivise the development of more sovereign cloud and AI computing services, something that PO2-A/B/C will do with different intensities. These options indirectly build on the Data Act's right to switch and multi-cloud, which all cloud service providers must enable and which all cloud users, including public administrations, can make use of, for example to switch to a sovereign service. In laying down and using a harmonized criteria for sovereign cloud and AI computing services, PO2-A/B/C build on an existing obligation of cloud service providers under the Data Act: To take technical, organisational and legal measures to prevent international and third-country governmental access and transfer of non-personal data held in the Union, outside of recognised international law enforcement cooperation, where this would conflict with Union or national law. The harmonized criteria for a sovereign service employed across PO2-A, B and C goes further by also capturing immunity to third-country policies affecting service continuity. This initiative thus does not create a new compliance burden for providers but rather enables those providers wishing for their services to reach a sovereignty label to build on existing compliance work under the Data Act. The AI Act already sets requirements for AI systems and general-purpose AI models ensuring a high-level protection of safety, health and fundamental rights, thus harmonising rules for the internal market. As detailed in annex 8, PO2-A/B/C and more generally CADA, focusses on cloud and AI computing services exclusively.

The Commission proposal for the Cybersecurity Act 2 empowers the Commission to impose prohibitions and mitigation measures by means of adopting implementing acts (1) prohibiting

specific types of NIS2 entities from using, installing or integrating ICT components from high-risk suppliers in key ICT assets; and (2) requiring such entities to apply targeted ICT supply chain mitigation measures, including supplier transparency obligations, restrictions on transfers or remote processing from third countries, third-party-audited technical safeguards, limits on outsourcing or supplier contracting, requirements for personnel vetting by national authorities, or diversification of supply. CADA relies on the CSA 2 for the exclusion of high-risk cloud and AI vendors from EU critical sectors. At the same time, CADA goes further than the CSA 2 and introduces a targeted approach to mitigating sovereignty risks specific to the provision and use of cloud and AI computing services. In defining what constitutes a sovereign service under PM11, PM15 and PM21, CADA leverages the future cybersecurity certification scheme for cloud services (EUCS), where the sovereignty levels under CADA require a gradual conformity against the EUCS assurance levels. There is no overlap between the requirements of the CADA sovereignty levels and the applicable requirements and those assessed under the EUCS, which covers exclusively technical cybersecurity aspects.

Figure 11. External coherence with most relevant ongoing legislative initiatives



In terms of **internal coherence**, all POs are designed to be coherent with the objectives of the EU and address the identified problem drivers (see also section 5.2.3). The measures under each PO are compatible with each other, see Annex 7. Sovereignty related measures respond to the needs of ensuring public order while the measures targeting critical dependencies focus on EU added value measures, notably in the context of innovation procurement. The promotion of open source solutions aims to build a foundation for auditable, open and interoperable services and products. The publicly auditable code provides a level of transparency and verifiability that is not possible in proprietary solutions, enabling authorities to independently assess security properties and verify the absence of undisclosed data flows or access mechanisms. Open source licensing removes the legal mechanisms that make vendor lock-in so difficult to escape in practice. The leverage that proprietary vendors have for the maintenance of the software is diminished with open source, reducing therefore the dependencies. The collaborative and distributed development models of open source create a form of supply chain resilience that is different from the proprietary solutions: open source communities distribute the maintenance and burden across a wide base of contributors, none of which can unilaterally determine the future of the project.

7.4. Subsidiarity and proportionality

As highlighted in sections 3.2 and 3.3, there is a clear need for action at EU level to address the identified problems and their drivers. All policy options respect the **subsidiarity** principle. In PO1-A, the Commission uses its convening powers to enhance the existing collaborative framework between Member States to stimulate compute capacity and remove deployment barriers. PO1-B contains EU-level rules but is designed with subsidiarity at its core since it entails decisions and financial incentives enforced at national level. PO1-C entails the most centralised EU action, with decisions and financial intervention enforced at EU-level, at the expense of less subsidiarity. In PO2-A, the EU's involvement is limited to be a mere convenor of national actors, hence highly respectful of subsidiarity. PO2-B requires more EU-level intervention, following a traditional Single Market logic through an EU-defined and Member State enforced sovereignty risk assessment mechanism, third-party audits, voluntary award criteria used for procurement of cloud and AI computing services in the public sector, and the vendor-neutral cloud and AI training programme. PO2-C adds further EU-level intervention, but in domains where no Member State can act alone, in particular as regards joint procurement. Moreover, it leaves to national authorities the ability to determine the sovereignty risk assessment outcome, while only producing guidelines to support a uniform implementation across MS.

All policy options are assessed to be **proportionate**, as EU-level action is limited to what is necessary to advance the EU's capacity, capability and autonomy in cloud and AI computing. PO1-A represents the lowest level of intervention and is less effective, while PO1-B entails the necessary and most effective EU-level intervention to address bottlenecks in the deployment of DCs by requiring that Member States implement national procedures. PO1-C is more ambitious and would entail additional administrative implications in terms of coordination with Member States. PO2-A introduces transparency measures that have limited prospects of changing current trends. It is proportionate to its ambition, as it imposes low compliance costs but its capacity to effectively achieve the intervention's objectives is limited. PO2-B further improves market openness with additional compliance mechanisms that would increase impacts and the expected benefits but may not be sufficient due to their voluntary nature. PO2-C is the most ambitious option as it proposes structural changes, through a tailored approach in existing public procurement practices and organised joint efforts. It is the most proportionate option given the magnitude of the problem and the intervention's goal to secure the necessary conditions for the Union's competitiveness and strategic autonomy. It strikes a balance between the need for effective sovereignty and the need to minimise unnecessary burdens. By establishing a granular framework with four levels of sovereignty, this option provides a nuanced and targeted approach to addressing the needs of both the public and private sectors. This tiered approach is justified, as it reflects the varying degrees of sensitivity and criticality of different use cases, and ensures that restrictions are proportionate to the risks involved. The addition of attestations of qualification to the Business Wallet of service providers and the establishment of a publicly available repository of qualified services facilitate transparency, reuse, and sharing among stakeholders.

7.5. Sensitivity analysis

The analysis has been designed to account for uncertainty and the multidimensional nature of policy impacts. As further detailed in Annex 4, a scenario-based sensitivity analysis was carried out to understand how the output of the cost-benefit analysis (CBA) behaves in response to changes in its inputs and assumptions. It was conducted to verify the uncertainty range (confidence interval) of the values estimated in the CBA for the most impactful policy measures. Given the different design, target stakeholders, and the type of impacts generated, the variables under scrutiny are not uniform or comparable. Therefore, rather than applying a full sensitivity

analysis, a bounded variation assessment was performed by introducing minimum and maximum variation to relevant parameters, thus creating worst and best case scenario for each measure[130].

7.6. Comparison per criteria

The following table synthesises the qualitative and quantitative analysis presented in Section 6, summarising the potential impacts of the policy options across economic, social and environmental dimensions.

Table 14. Summary of economic, social and environmental impact of the Policy Options, relative to the baseline

Criteria	PO1-A	PO1-B	PO1-C	PO2-A	PO2-B	PO2-C
Economic impact	+	+++	++	+	++	+++
Social impact	+	++	-	+	++	+++
Environmental impact	+	-	++	o	+	+

Legend: o neutral impact; + minor positive; ++ positive; +++ significant positive; - minor negative; -- negative impact; --- significant negative, all with respect to the baseline

With respect to their **economic impact**[131], PO1-B and PO2-C are expected to deliver the strongest outcomes, mainly driven by long-term benefits due to accelerated infrastructure development, joint procurement and cloud federation among Member States. PO1-A delivers only modest benefits, limited to administrative simplification and minor efficiency. By issuing guidelines and reinforcing the current collaborative framework between data centre developers, cloud service providers, energy actors, public authorities and other relevant stakeholders, the option would reduce some uncertainty around data centre planning and deployment. Data centre operators and authorities would benefit from greater predictability in permitting and common engagement. However, because this option would not introduce binding legal changes, dedicated support or formal deployment mechanisms, its impact on investment decisions would remain modest. In terms of innovation and technological sovereignty, this option could help create a more predictable environment for data centre development but would not change Europe's ability to scale cloud computing capacity. Wider economic effects would also be positive but limited, considering the reduced friction, better information flows and improvements in investment conditions. PO1-B is expected to have a more significant economic impact, as it would generate the strongest infrastructure related economic benefits, driven by increased computing capacity. By promoting legislative and financial measures in the form of project facilitators for data centre deployment, areas for fast-track sustainable development, possible national funding mechanisms for priority projects and monitoring of capacity, this option would create stronger incentives for investment. Reducing delays linked to data centre deployment would consequently decrease their time to market and potentially further crowd in private investment. For data centre operators the main benefits would stem from more predictable permitting procedures, clearer administrative pathways and potentially lower risks. Increased attractiveness of the Union for investment decisions would also help address regional capacity gaps. For public authorities, this option would involve higher administrative responsibilities than PO1-A, as they would need to designate these zones and contribute to setting up project facilitators. These costs are expected to be offset by broader economic benefits, including increased investment, job creation and local infrastructure development. This would also contribute to strengthen the infrastructure based needed to develop cloud solutions, AI and support digitalisation in the public and private sector. Under this option

[130] This reflects the structure of the standard cost model used for most of the policy measures, which relies on a limited number of inputs, thus limiting the interpretability of traditional one-at-a-time sensitivity testing.

[131] The scoring of economic impacts reflects the estimated costs and benefits associated with each policy option, but also their broader effects on industry (including SMEs), public authorities, innovation and technological sovereignty, possible wider economic effects, trade, and the functioning of the internal market.

the Commission's role would focus on monitoring capacity, supporting coordination across Member States and ensuring consistency with other EU-level objectives. PO1-C also produces gains through EU-level fast-tracking and funding, but these remain below PO1-B due to smaller expected time savings and a more centralised implementation, which is expected to reduce its effectiveness. The evidence collected suggests that the expected economic benefits under this option would be weakened by implementation delays due to the additional coordination and governance arrangements. For operators this would reduce the value of EU-level deployment and support. For public authorities, the option could offer long-term benefits by creating a more coherent EU-level mechanism for data centre deployment. However, the need to coordinate at EU level is expected to create administrative complexity, as national authorities would still need to be involved in permitting, zoning, energy coordination, environmental assessments and local processes, including community engagement. The option could still have a relevant economic impact but the evidence collected suggests that this would be slower to materialise and less effective in addressing deployment bottlenecks and national decision making procedures. PO2-A yields limited economic benefits by increasing transparency and visibility of sovereign cloud and AI computing services, with overall net costs aggregated across stakeholders. For cloud service providers, especially smaller European ones, this option could still reduce barriers to market entry and help users better understand available services. However, due to the non-binding nature of the measures, the impact on actual demand and procurement behaviour would be limited. Similarly, the impact on technological sovereignty would be positive but modest, contributing the overall positive but minor economic impact of this option. PO2-B is expected to improve economic outcomes by reducing cross-border compliance costs and increasing trust in sovereign services, generating net benefits. Providers would be able to leverage the voluntary frameworks to create reputational and market benefits. Wider economic benefits are expected and could include increased demand for sovereign services and overall stronger market competition. However, while recognising the positive economic impact of the option on different stakeholders, its effectiveness in achieving these results would ultimately depend on market uptake and public sector adoption. PO2-C builds on PO2-B and is thus expected to deliver the largest economic impact, despite higher costs. The sovereignty risk assessment is expected to enable a once-only audit process across MS with significant savings for providers, whereas the joint procurement and federation mechanism are expected to enable savings for authorities procuring cloud and AI computing services and exchanging their idle compute capacity. The impact of this option on innovation and technological sovereignty is expected to be substantial. By using public demand strategically, the public sector could support the development and scaling of sovereign cloud and AI computing services, while still leaving to non-European providers a relevant share of the market, based on MS needs and individual assessments. Wider economic effects would include increased competition, higher productivity through broader adoption of advanced cloud and AI computing services, greater resilience of digital supply chains and stronger opportunity for European SMEs. While direct economic impacts were more robustly quantifiable, **social impacts** were not monetised due to the absence of data on willingness to pay or stated preferences. The impacts considered include differences in employment, skills development, and public acceptance of the different options. PO1-B in combination with PM8 and PM9 is expected to produce the best outcome among the first set of options, especially in terms of additional employment created and public acceptance of new data centre projects. The option empowers local authorities in siting decisions, thus fostering decision-making processes closer to citizens. Positive social impacts are also expected as this option focuses on shaping data centre development towards sustainable, innovative and strategic projects, e.g. facilities contributing to tangible community benefits such as waste heat reuse and overall development of local economies. Conversely, PO1-A delivers

limited engagement gains, while PO1-C weakens perceived proximity to decision-making. For cloud and AI services, PO2-B and PO2-C address skills shortages and employability, supporting broader societal acceptance of technological sovereignty. Finally, **environmental impacts** were assessed in environmental terms but not monetised to ensure consistency across impact categories and avoid bias from uncertain valuation assumptions. In this context, PO1-C would achieve the strongest performance by combining efficiency-driven innovation, sustainable siting, and renewable integration, substantially reducing emissions intensity while limiting energy growth. By contrast, PO1-B's capacity expansion outweighs efficiency gains, resulting in the highest absolute increases in electricity demand and CO_2 emissions. PO2-B and PO2-C provide modest environmental benefits through improved server utilisation and reduced duplication of infrastructure under the cloud federation.

The multi-criteria analysis (MCDA) was used to complement the CBA by integrating survey-based evidence on the perceived effectiveness of the measures, as well as their expected environmental and social impacts. It provided an alternative analytical lens, particularly through its underlying components, i.e. stakeholder responses of the proposed measures. The aggregate results were interpreted with caution, as they reflect the original configuration of measures and options, which was partly superseded by subsequent refinements. Overall, the weighted aggregate scores across the different assessment dimensions confirmed the consistency of the initial comparative assessment (see annex 4 section 6). With respect to Problem 1 - limited and geographically concentrated availability of computing capacity in the EU - economic operators showed a preference for PO1-B over PO1-C. Similarly, PO1-B scores higher for national public authorities, driven mainly by better cost outcomes and perceived social and environmental effects. With respect to Problem 2 - Dependence on cloud and AI computing services supplied by non-European providers – the results pointed to a clear preference for PO2-C because of its expected economic and social benefits, including potential effects on transparency and citizen trust. On the other hand, national public authorities appeared to favour PO2-B due to the voluntary nature of most of the measures. This should be nevertheless interpreted with caution as national authorities represented a limited share of survey responses, which may have affected the robustness of the aggregate scores.

Table 18 compares the different POs against the criteria presented in Section 7, summarising the relative performance of each option against the baseline scenario in terms of effectiveness, efficiency, coherence, subsidiarity and proportionality.

Table 15. Comparison of the options per criteria, relative to the baseline[132]

Criteria	PO1-A	PO1-B	PO1-C	PO2-A	PO2-B	PO2-C
Effectiveness	+	+++	++	+	++	+++
Efficiency	–	+++	+++	–	+++	++++
Coherence	++	+++	++	++	++	+++
Subsidiarity and proportionality	+++	+++	++	+++	++	+++

Legend: o no relevance; + more effective/efficient/coherent/proportionate than the baseline; +++ much more effective/efficient/coherent/proportionate than the baseline; - less effective/efficient/coherent/proportionate than the baseline; --- much less effective/efficient/coherent/proportionate than the baseline

PO1-A's soft measures contribute to making it a cost-effective and coherent option but limit its effectiveness, as it contributes to the specific and general objectives only to a limited extent with respect to the status quo. PO1-B's administrative simplification and fast-track areas strengthen its

[132] "+" (more effective/efficient/coherent/proportionate than the baseline) to "+++" (much more effective/efficient/coherent/proportionate than the baseline); from '-' (less effective/efficient/coherent/proportionate than the baseline) to '---' (much less effective/efficient/coherent/ proportionate than the baseline).

effectiveness by achieving the greatest expected increase in compute capacity and reduction of bottlenecks for DC deployment, while being proportionate to solve the issue and leaving implementation within Member States. PO1-C's EU-level measures improve effectiveness and efficiency, given the EU-level centralisation of efforts, but constrain subsidiarity through centralised enforcement. PO2-A improves effectiveness in reaching the specific objectives but presents overall net costs and falls short of the challenge at hand. PO2-B's design balances coherence and efficiency, while achieving only moderate effectiveness given the magnitude of the problems to be addressed and the voluntary nature of its measures. By encouraging rather than mandating a gradual shift towards more sovereign solutions in the public sector, PO2-B may accelerate some porting and migration costs for users and providers, although they are expected to remain relatively contained and market-driven. Finally, PO2-C generates strong synergies across all criteria, with the highest costs and savings over ten years, reflecting high ambition at the expense of increased operational complexity. It is likely to accelerate porting and transition costs more significantly, particularly for entities deciding to move workloads and applications to the highest levels of sovereignty assurance. While the option could increase operational complexity and short to medium-term costs, it would be more proportionate and coherent than other options as it matches the scale of the interventions to the nature of the challenge. Moreover, the expected upfront and operational costs should still be weighed against long-term and less easily quantifiable benefits, including reduced strategic dependencies, increased control over critical digital infrastructure, improved resilience and greater European technological sovereignty.

8. PREFERRED OPTION

8.1. Outcome of comparison of policy options

Structuring the policy options into blocks addressing individual problems has allowed to evaluate the most effective, efficient, and proportionate measures from each block of options, while also analysing the package's comprehensiveness in addressing both problems and their underlying drivers. This section brings together the evidence across criteria to assess the relative merits of the policy options in addressing the identified problems and objectives.

For the first problem**,** PO1-B performs as the option that most effectively improves the limited availability of computing capacity in the EU relative to the baseline and alternative options. Administrative streamlining and fast-track permitting at national level, coupled with strategic funding and monitoring of capacity, appear as the most impactful options to tackle the bottlenecks for expanding such capacity in the EU. The option is expected to generate greater benefits than costs for both private sector and public sector stakeholders. Moreover, public acceptance of data centres is expected to be highest because local authorities would have a stronger role in decisions on where and how they are built. This means that decisions would be made closer to the people affected by them. By contrast, PO1-C is expected to reach a lower level of computing infrastructure deployment than PO1-B, because PM10 adds a layer of decision-making at EU-level. Nevertheless, PO1-C reaches the best environmental impact due to the expected positive contribution of EU-level funding (PM8 and PM9) to R&D and innovation in sustainable technologies. Given the importance of fostering deployment of data centres with a focus on sustainability and reducing environmental impacts, **for the first problem, the analysis points towards a package centred on PO1-B, supplemented by PM8 and PM9** as a proportionate response. This combination is expected to offer a favourable balance between supporting deployment of capacity and better energy efficiency and environmental performance per unit of new capacity.

With respect to the second problem, PO2-C emerges as the best performing option across the comparison criteria. Through clarity in the definition of sovereignty, which is also defined in a

proportionate manner, combined with complementary measures addressing procurement and open source, it will facilitate the uptake of solutions that meet desired sovereignty levels, and provide opportunities for European providers. It incorporates, in an incremental way, several elements of the other PO2 policy options. Additional individual PMs are expected to deliver only limited marginal gains: PM12 and PM13 are soft measures that the Commission could decide to undertake in the future should the need arise; PM14 lacks perspective on how effective the enforcement of the Data Act will be (see annex 4). **On this basis, PO2-C is retained as the preferred package addressing the second problem.**

As outlined above, the first set of options primarily addresses SO1 and SO2, while the second set is more directly aligned with SO3 and SO4. Given this differentiated contribution, a combined application of the best performing options among the two sets is expected to be the most effective approach to tackle the **full range of problems and underlying drivers** identified in the problem definition, which are heterogeneous in nature. Taken together, these options would also support the achievement of the **general objective** of ensuring the functioning of the internal market for cloud and AI computing services and securing the necessary conditions for the Union's competitiveness and strategic autonomy, by providing a coherent response to the interconnected challenges identified. Therefore, with regards to **effectiveness**, the preferred package is expected to address the identified problem drivers in a comprehensive manner and, relative to the baseline, achieve a "very effective ("+++") score against all Specific Objectives.

	SO1: Increased computing capacity	**SO2:** Conditions for sustainable and innovative capacity	**SO3:** Decreased reliance on non-EU providers	**SO4:** Enhanced resilience of supply of cloud and AI computing services
Policy option 1A	+	++	*n.r.*	*n.r.*
Policy option 1B	+++	+++	*n.r.*	*n.r.*
Policy option 1C	++	++	*n.r.*	*n.r.*
Policy option 2A	+	*n.r.*	+	+
Policy option 2B	+	*n.r.*	++	++
Policy option 2C	++	*n.r.*	+++	+++
Preferred Package	+++	+++	+++	+++

The retained package is hence made of the following policy measures:

PO1-B:

- PM4 - National facilitator
- PM5 - Fast-track areas
- PM6 - National funding support
- PM7 - Deployment targets
- PM8 - EU R&D funding
- PM9 - EU deployment funding for strategic projects

PO2-C:

- PM19 - Mandatory award criteria (which builds over PM16)
- PM20 – Open Source use in the public sector
- PM21 – Mandatory sovereign risk assessments for the use of cloud and AI computing services (which builds over PM11 and PM15)
- PM22 – Joint EU-level procurement of cloud and AI (which builds over PM17)
- PM23 – SME cloud and AI support scheme (which has synergies with PM18)
- PM24 – Cloud and AI toolbox

Overall, the analysis suggests that PO1-B and PO2-C perform relatively strongly in terms of **economic and social benefits**, while PM8 and PM9 play an important role in supporting **environmental sustainability**. This highlights the importance of combining such options to balance growth, sovereignty, and climate objectives in a balanced manner.

This package combining PO1-B, PM8 and PM9, is expected to generate **positive efficiency effects**, as the expected benefits in the short and medium term seem to outweigh the generated costs over the assessment period for different stakeholders. The main expected benefits under PO1-B arise from the measures that simplify procedures and reduce fragmentation across Member States. Similarly, under PO2-C key benefits are expected for public authorities under the joint procurement scheme and the federation of capacity. These are altogether expected to reduce administrative burdens, shorten timelines and improve legal certainty for private operators and public authorities. This combination of options also entails implementation and transition costs. There are mainly linked to adapting systems and procedures, familiarising stakeholders with the new requirements and ensuring compliance. Most of these costs are one-off or transitional in nature, while several of the expected benefits are recurring over time. This combination of options is expected to deliver a positive balance of costs and benefits, while achieving the objectives in a proportionate and cost effective manner.

In terms of **coherence**, the package is consistent with the policies described under section 1.2. The analysis does not indicate significant overlaps, as the measures tackle the DC, cloud and AI markets from different perspectives. Instead, they address the objectives pursued, while securing the EU's digital competitiveness and resilience.

This package is also respectful of **subsidiarity and proportionality** principles. While Member States in principle can enact at national level many of the measures, both problems addressed are characterised by common underlying drivers across the EU and would require a degree of coordination and harmonisation that cannot be ensured through national action only. EU-level intervention is therefore expected to offer clear added value, as the objectives of this initiative seem impossible to be achieved sufficiently by Member States alone. At the same time, the achievement of the expected impacts will be shaped by national implementation choices and contextual factors, underlining the key role of Member States in materialising the initiative.

The MCDA was also used to examine the options and measures from an additional perspective. While it assessed the options separately for each problem area, it provided a wat to consider their performance across effectiveness, environmental and social impact dimensions. This approach allowed us to capture additional social and environmental effects, for which robust monetary valuation such as willingness to pay or shadow price estimates, was not available.

8.2. Application of the "One In One Out" (OIOO) Approach

The preferred policy package is expected to lead to both administrative cost savings and administrative costs for businesses and national public authorities. The details of how these administrative costs and savings have been quantified, including the underlying assumptions can be found in Annex 4, section 3. The table below summarizes the main administrative costs and savings, including details on the related activities, who is affected and their quantification.

Table 16. Application of the OIOO approach - Businesses

Preferred package	Activities	Economic operators affected	Monetization (NPV 2027 – 2036)
PO1-B PM5*	One-off administrative costs of preparing the application file to access the fast-track areas	Data centre operators	EUR 0.8 – 2.8 m
PO1-B PM6	One-off administrative costs of preparing the application to respond to the calls (est.12 applications every two years)		EUR 0.2 – 1.3 m
PO1-B PM7	Recurrent administrative costs of survey response time and eventual periodic verification of data on compute capacity		EUR 0.2 – 0.6 m
PM8	One-off administrative cost of preparing the	Data centre	EUR 0.7 – 1.6 m

Preferred package	Activities	Economic operators affected	Monetization (NPV 2027 – 2036)
	application under calls for proposals (est. 20 applications every two years)	operators	
PM9	One-off administrative cost of preparing the application under calls for proposals (est. 15 proposals every two years)	Data centre operators	EUR 0.4 – 1.2 m
PO2-C PM19	Recurrent administrative costs of adapting the offers to the new criteria	Cloud and AI service providers	EUR 13.6 – 96.4 m
PO2-C PM21	Recurrent administrative costs for new audits at assurance level 2 - 4	Private sector (independent auditors)	EUR 4.4 – 4.4 m
PO2-C PM21	Recurrent administrative costs for audit renewals at assurance level 2 - 4	Private sector (independent auditors)	EUR 7 – 7 m
PO2-C PM21	Recurrent administrative costs of intermediate audits at assurance level 2 - 4	Cloud and AI service providers	EUR 53.9 – 134.8 m
PO2-C PM21	Recurrent administrative burden for private sector entities under NIS 2 Annex 1 to address non-technical risks	Private sector entities operating in sectors listed under Annex I of NIS2	EUR 480– 2 620 m
PO2-C PM21	Recurrent administrative **cost savings** in intermediate audits from doing it once for all 27 MS	Cloud and AI service providers	EUR 404.3 – 2 021.4 m
PO2-C PM23	One-off administrative cost of preparing the application under call for applications (est. 16,000 applications per year)	SMEs	EUR 27.7 – 83.4 m

**PM4 and PM5 are expected to generate reduced administrative burdens and improved information through more consistent and predictable interactions with permitting bodies. However, these administrative savings have not been monetised due to the lack of robust data and their relative smaller scale compared to the economic benefits captured through the NPV approach.*

Table 17. Application of the OIOO approach - Public Administrations

Preferred Package	Activities	**Monetization** (EUR, NPV 2027 – 2036)
PO1-B PM4	Recurrent administrative burden reduction thanks to the project facilitator which would reduce parallel processing and back-and-forth interactions	EUR 83.1 – 138.6 m
PO1-B PM5	One-off administrative costs for drafting the strategies for national data centre deployment	EUR 1.2 – 6.1 m
PO1-B PM5	Recurrent administrative costs of mapping the fast-track areas and updating the strategies	EUR 46.4 – 86.3 m
PO1-B PM5	Recurrent administrative burden reduction thanks to the fast-track areas with additional reduction in parallel processing and reporting duties	EUR 83.1 – 138.6 m
PO2-C PM19	Recurrent administrative cost savings from using standard non-specific award criteria when drafting the specifications	EUR 4.3 – 13.1 m
PO2-C PM19	One-off administrative cost to update the procedures related to the public procurement of cloud and AI computing services and draft plans on highly critical use cases involving the purchase of sovereign services	EUR 3.4 – 13.5 m
PO2-C PM19	Recurrent administrative costs to update the plans and track their progress	EUR 46.4 – 115.4 m
PO2-C PM20	One-off administrative costs to adapt the procurement templates to promote open source	EUR 6.9 – 13.9 m
PO2-C PM20	Recurrent administrative costs to maintain the Open Source Programme Office each year	EUR 60.5 – 211.7 m
PO2-C PM21	Recurrent cost savings from using the sovereignty scheme in tenders	Around EUR 2.5 m
PO2-C PM21	Recurrent administrative costs from validation of the audited services and renewals	EUR 0.3 – 0.8 m

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The Commission (DG CONNECT) will be responsible for monitoring the implementation of the intervention on a regular basis, possibly with the support of other Commission services, EU agencies, external studies, Member State and market data. A set of possible indicators is provided in the following table, alongside preliminary questions for the evaluation of the intervention, which is expected five years after implementation. Annex 11 presents the detailed monitoring framework devised for this intervention and how this will build upon existing schemes to avoid duplication and benefits from synergies.

With respect to the expected targets of the intervention, the data provided in this assessment presents indicative ranges, which should be interpreted as plausible trajectories. In line with the Better Regulation Toolbox, quantitative targets were based on the problem analysis, baseline scenario, available evidence from the assessment, including validation through interviews, and the expected scale of policy impact. They were defined to quantitatively measure the effectiveness of the intervention in the next years and paired with indicators for a systematic review. They included a clear timeframe, i.e. by 2030 or 2035, expectations based on the evidence gathered and the availability of data collection systems to make this monitoring effective.

Table 18. Summary of KPIs by Specific Objective

Operational objectives and performance thresholds	Possible indicators for monitoring/evaluation	Main data sources and data collection methods
Increase computing capacity deployed in the EU through innovative and sustainable technologies: By 2030, +200% EU computing capacity vs 2025 and ensuring that such capacity fully covers its needs by 2035[133]; ≥25% of global share[134]; energy-efficient technologies in ≥80% of new facilities[135].	• Installed computing capacity (MW IT load) by MS • Aggregate general purpose and AI-optimised compute, shifting to a measurement by FLOPs as opposed to MW. • EU share of global installed computing capacity • Number of new EU-based DCs operational per year • Utilisation rate of EU computing capacity; measures on PUE, WUE, location-based emissions and related environmental impact of data centres • Deployment of innovative and energy-efficient technologies (pilots launched and uptake of new solutions) • Share of renewable energy in data centres and waste-heat reuse • Total annual public and private investment in EU-based DCs • Share of new data centre capacity deployed outside existing hubs and in underserved regions	Survey (and follow-up interviews) of data centre operators, national authorities and TSOs/DSOs Desk research EED reporting Interviews with experts, academia, think tanks and associations Industry dataset, e.g. Data Centre Map, EUDCA EEA emission data
Ensure attractive conditions for the deployment of	• Average permitting time for new data centre projects	Surveys per (and follow-up interviews) across

[133] Since the precise level of self-sufficiency is impossible to anticipate today, PM7 has been conceived to monitor the evolution of supply and demand of computing capacity across EU Member States.
[134] This 25% target of EU-27 global share has been derived from the estimated increase in EU capacity expected under PO1-B. Under the baseline scenario, the EU-27 share of global data centre capacity is projected to grow from 20% (2025) to 23% (2030), i.e. reaching around 28 GW in 2030. This is based on the Goldman Sachs forecast that total global data centre capacity will reach around 122 GW by 2030. The additional capacity expected to be enabled by the proposed measures could raise this EU share to around 27% by 2030. To account for uncertainties, a more conservative threshold of 25% was set to capture the additional percentage points of global capacity.
[135] The need to prioritise and have energy-efficient technologies in at least 80% of new installations, measured by PUE, WUE and other relevant indicators, is considered a necessary threshold to comply with EU goals of climate neutrality by 2050.

Operational objectives and performance thresholds	Possible indicators for monitoring/evaluation	Main data sources and data collection methods
sustainable and innovative computing capacity: By 2030, overall permitting time should be <18 months[136], +30% annual investment vs. 2025[137], ≥20 MS with harmonised frameworks[138].	• Total administrative burden for operators • Share of projects delayed/cancelled due to regulatory or infrastructure barriers • No. of MS with simplified permitting frameworks • Cost competitiveness index (€/MW build cost, €/MWh energy cost vs. US/Asia)	national authorities and operators FDI statistics Eurostat
Decrease the overall reliance on non-European cloud and AI computing services: By 2035, ≥ 30% market share of EU-homegrown cloud and AI computing service providers in the EU, i. e. at least doubling it against the baseline	• Share of total EU cloud and AI computing services revenue captured by European service providers • Number of public sector authorities served by sovereign providers per MS • Share of installed EU DC capacity owned by European providers • Share of idle capacity shared among MS	Survey (and follow-up interviews) of data centre operators and national authorities Desk research Market research
Contribute to the protection of public order by enhancing the resilience of supply of cloud and AI computing services, in particular in the public sector: By 2035, 100% of highly critical use cases in the public sector operated using sovereign cloud and AI computing services[139]	• Number of cloud and AI services audited under level 2, 3 or 4 • Compliance rate by contracting authorities (%) with the sovereignty scheme • Annual value of EU public procurement of sovereign cloud and AI computing services • SME share (%) in awarded public contracts • Number of public sector solutions released as open source in the repository, and their downloads by third parties	Number of assessed and evaluated sovereign services in the repository Survey (and follow-up interviews) of DC operators and national authorities Desk research Market research TED data

Table 19. Preliminary questions for the evaluation of the intervention

Evaluation criterion	Assessment objective and possible evaluation questions
Effectiveness	**Goal:** assess the extent to which the objectives of the initiative have been achieved and how benefits have accrued to different stakeholders. *To what extent did the intervention increase EU installed computing capacity and create the conditions for easier data centre deployment? How did it foster the development and deployment of innovative and sustainable data centres and a better use of energy sources? To what extent did it increase clarity around the concept of sovereign cloud and AI computing services? How did it improve the market share of European cloud and AI computing service operators? What is their market share for sovereign use cases? To what extent did it increase federated resources across the public sector and joint procurement for cloud and AI computing services? To what extent did it increase the use of open source solutions?*
Efficiency	**Goal:** assess the extent to which the initiative has been cost-effective, analysing the relationship between expected and actual benefits and costs. *Have benefits and cost savings been achieved at proportionate costs for different stakeholders?*

[136] This has been set to ensure that regulatory procedures for deploying data centres across the EU are reduced in a consistent way. Under the baseline, average permitting duration was estimated to be of 32 months across the 12 Member States under scrutiny. Reducing this timeline to 18 months is a realistic improvement, even if still above today's best-performing countries.
[137] Reducing administrative barriers has been shown in the literature, and confirmed through interviews, to greatly improve project bankability and attract additional investments. Hence, a 30% additional investment unlocked compared to the baseline scenario has been set as a reasonable success criterion. This should be measured against the additional capacity deployed.
[138] The objective of seeing 20 Member States with harmonised frameworks stems from a willingness to improve visibility and simplify market access to data centre investors and businesses, so that they can fully exploit the Single Market without additional administrative burdens.
[139] Since the objective consists in enhancing the resilience of supply of cloud and AI computing services, in particular in the public sector, a long-term target of full compliance is expected as a measure of success.

Evaluation criterion	Assessment objective and possible evaluation questions
Relevance	**Goal**: assess the extent to which the objectives of the initiative still reflect current and future needs. *To what extent the initiative still addresses relevant needs? How is it still aligned with EU priorities?*
Coherence	**Goal:** assess the initiative's internal and external coherence, i.e. if the different elements of the intervention worked together to reach the set goal and if it worked well or overlapped with other initiatives, both at EU level and national level. *To what extent is the initiative consistent with existing and future energy, digital, competition, environmental, security rules at EU level and national level?*
EU Added value	**Goal**: assess the extent to which the initiative brought EU added value compared to what could have been achieved by Member States alone. *To what extend did EU-level action prevent fragmentation of DC rules? How did it improve cross-border service delivery and competitiveness of EU providers?*

ANNEX 0 - ENDNOTES

[i] The Draghi Report on competitiveness
[ii] Draghi report
[iii] Competitiveness Compass
[iv] JOIN/2023/20 final
[v] Mission letter to EVP Virkkunen

[vii] The AI Continent Action Plan | Shaping Europe's digital future
[viii] Europe's digital decade: 2030 targets | European Commission
[ix] REPORT on European technological sovereignty and digital infrastructure | A10-0107/2025 | European Parliament
[x] Council Conclusions of 5 December 2025
[xi] Federal Cloud Computing Strategy, February 2011?
[xii] See for example Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing?
[xiii] America's AI Action Plan
[xiv] Accelerating Federal Permitting of Data Center Infrastructure – The White House
[xv] Promoting The Export of the American AI Technology Stack – The White House
[xvi] China plans network to sell surplus computing power in crackdown on data centre glut | Reuters
[xvii] UK Compute Roadmap - GOV.UK
[xviii] UAE Dominates Global Data Centre Rankings as Region Becomes Digital Infrastructure Hotspot -MIT Sloan Management Review Middle East
[xix] Decision - 2022/2481 - EN - EUR-Lex
[xx] Directive - 2023/1791 - EN - EUR-Lex
[xxi] Regulation – 20200/852 – EN – EUR-Lex
[xxii] Regulation - 2019/424 - EN - EUR-Lex, which is currently under review.
[xxiii] Digital Networks Act, information accessed from the 'Have Your Say' page
[xxiv] Commission collects views in preparation of the European Grids Package - European Commission
[xxv] Savings and investments union - Finance - European Commission
[xxvi] Apply AI Strategy | Shaping Europe's digital future
[xxvii] Data Act
[xxviii] Regulation - 2022/1925 - EN - EUR-Lex
[xxix] Regulation - EU - 2024/1689 - EN - EUR-Lex
[xxx] Cybersecurity Act (CSA)
[xxxi] Regulation - 2022/2554 - EN - DORA - EUR-Lex
[xxxii] Directive on Security of Network and Information Systems (NIS2)
[xxxiii] Public Procurement Directive
[xxxiv] Cloud Services Market to Exceed 68 Billion in 2010 | Security Magazine
[xxxv] Gelvanovska-Garcia, Natalija; Mačiulė, Vaiva; Rossotto, Carlo Maria. 2024. Advancing Cloud and Data Infrastructure Markets: Strategic Directions for Low- and Middle-Income Countries. Sustainable Infrastructure Series. © World Bank. http://hdl.handle.net/10986/41587 License: CC BY 3.0 IGO.
[xxxvi] 53% EU enterprises used paid cloud services in 2025 - News articles - Eurostat
[xxxvii] European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group
[xxxviii] European IT providers struggle to capitalise on continent-wide growth in cloud demand | Computer Weekly
[xxxix] European industrial technology roadmap for the next generation cloud-edge offering, May 2021. Available at: https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf
[xl] CIA Awards Secret Multibillion-Dollar Cloud Contract; CIA awards multibillion C2E cloud contract to AWS, Microsoft, Google, Oracle, and IBM.
[xli] What made AWS the leader in the cloud industry?
[xlii] Training and Certification for AWS Partners | Digital and Classroom Training | AWS; Top 10 AWS Consulting Partners; Azure Partners – Find an Azure Expert Partner | Microsoft Azure; Microsoft partnerships drive innovation

and growth in Europe in times of uncertainty – Microsoft Pulse; Cloud Solution Provider program overview - Partner Center | Microsoft Learn;

[xliii] Cloud computing - statistics on the use by enterprises - Statistics Explained - Eurostat

[xliv] Netflix, Prime Video and Disney+ have 85% of Europe's SVOD market - Mobile Europe

[xlv] European IT providers struggle to capitalise on continent-wide growth in cloud demand | Computer Weekly

[xlvi] Grassano, N., Hernandez Guevara, H., Tuebke, A., Amoroso, S., Dosso, M., Georgakaki, A. and Pasimeni, F., The 2020 EU Industrial R&D Investment Scoreboard, EUR 30519 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978- 92-76-27418-6, doi:10.2760/203793, JRC123317. Available here: SB2020_final_16Dec2020_online.pdf.

[xlvii] The Future of Hyperscaler Capital Expenditures: A Deep Dive into AI and Cloud Computing – HyperFRAME Research

[xlviii] See also Arnal, J. (2025). Towards Competitive Cloud Ecosystems: Strategic Responses for Europe's Digital Future, IE Center for the Governance of Change. Available here: CGC_Competitive_Cloud_Ecosystems_2025.pdf

[xlix] Crémer, Jacques & Biglaiser, Gary & Mantovani, Andrea, 2024. "**The Economics of the Cloud**," TSE Working Papers 24-1520, Toulouse School of Economics (TSE).

[l] The UK's Competition and Markets Authority detail this situation in their July 2025 report

[li] Market study into cloud services | ACM

[lii] Gartner Says Worldwide Sovereign Cloud IaaS Spending Will Total $80 Billion in 2026

[liii] AI and Compute; The cost of compute power: A $7 trillion race | McKinsey; How Can We Meet AI's Insatiable Demand for Compute Power? | Bain & Company; AI to drive 165% increase in data center power demand by 2030 | Goldman Sachs; The 2025 AI Index Report | Stanford HAI

[liv] Statista Technology Market Insights, 2025. Available here: Artificial Intelligence - EU-27 | Statista Market Forecast

[lv] Data Centres | CBRE

[lvi] Global Data Center Trends 2025 | CBRE

[lvii] Big Tech's AI investments set to spike to $364 billion in 2025 as bubble fears ease?

[lviii] Technopolis Group et al. (2025), "Study: Cloud and AI".

[lix] Technopolis Group et al. (2025), "Study: Cloud and AI".

[lx] KPMG | The evolving data centre landscape

[lxi] Data coming from the Cloud and AI Study. Additional data can be found here: Financing Infrastructure for a Competitive European AI - Groupe d'études géopolitiques

[lxii] Technopolis Group et al. (2025), "Study: Cloud and AI".

[lxiii] Savills | Costs on the rise

[lxiv] Unlocking the European AI revolution | McKinsey

[lxv] Data Centres | CBRE

[lxvi] Data Centres | CBRE

[lxvii] RTE | No new data centres for the capital for the foreseeable future

[lxviii] HOW DATA CENTERS HAVE COME TO MATTER: Governing the Spatial and Environmental Footprint of the 'Digital Gateway to Europe' - Monstadt - 2025 - International Journal of Urban and Regional Research - Wiley Online Library

[lxix] CREOS annual report 2021

[lxx] ServerMania | Cloud server prices

[lxxi] Mistral AI warns of lack of data centres and training capacity in Europe | Euronews

[lxxii] Public Cloud - EU-27 | Statista Market Forecast

[lxxiii] Cloud is a Global Market - Apart from China | Synergy Research Group

[lxxiv] European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group

[lxxv] European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group

[lxxvi] European Software and Cyber Dependencies

[lxxvii] Competition in the provision of cloud computing services (EN)

[lxxviii] Asterès | Technological dependence on American Software and Cloud services

[lxxix] ChatGPT in the Public Sector - overhyped or overlooked?

[lxxx] AI in Europe: A new opportunity for growth | McKinsey

[lxxxi] Understanding cloud outages: Causes, consequences and mitigation strategies | HCLTech

[lxxxii] What the EU Needs to do to Challenge Big Tech Cloud Dominance | TechPolicy.Press; Amazon web services return to 'normal operations' after mass outage, tech giant says - BBC News.

[lxxxiii] Nicolas Guillou, French ICC judge sanctioned by the US: 'You are effectively blacklisted by much of the world's banking system'
[lxxxiv] Kyndryl announces agreement to purchase cloud-services provider Solvinity
[lxxxv] Ibid
[lxxxvi] Dutch parliament calls for end to dependence on US software companies | Reuters
[lxxxvii] ECB Guide on outsourcing cloud
[lxxxviii] Microsoft Can't Keep EU Data Safe From US Authorities
[lxxxix] Section 3 - Capgemini. Cloud Sovereingy: the road ahead
[xc] Page 43 to 47 - Baromètre de la cybersécurité des entreprises du CESIN,
[xci] How Many Data Centers Are in the US? Latest Statistics and Trends - C&C Technology Group
[xcii] Recent Trends in U.S. Services Trade: 2022 Annual Report
[xciii] Global Infrastructure Regions & AZs
[xciv] Discover more about regions and availability zones | OVHcloud Worldwide
[xcv] OECD (2025), "Competition in the provision of cloud computing services", *OECD Roundtables on Competition Policy Papers*, No. 323, OECD Publishing, Paris, https://doi.org/10.1787/595859c5-en, pp. 23-24.
[xcvi] Oaktree-backed firm unveils $1.2 billion Amsterdam 'hyperscale' data centre project | Reuters
[xcvii] https://www.mordorintelligence.com/industry-reports/europe-colocation-market-industry
[xcviii] Data Centres | CBRE
[xcix] Leitmotiv - Toward our Digital Future
[c] Google raises 2025 capex estimate, again, to $91-93bn - plans "significant increase" in data center spend for 2026 - DCD
[ci] OVHcloud - Results
[cii] Too late to act? Europe's quest for cloud sovereignty | Clingendael
[ciii] NGP Capital | The Cloud Evolution: From Hyperscaler Dominance to Modular Infrastructure
[civ] See here: Announcing the Regional 2024 AWS Partners of the Year for Europe, Middle East, and Africa?
[cv] See for instance AWS Distribution program or Microsoft's partner program
[cvi] The economics of the Cloud – Toulouse School of Economics – March 2024
[cvii] Partnerships Between Cloud Service Providers and AI Developers
[cviii] Competition in the provision of cloud computing services (EN); Partnerships Between Cloud Service Providers and AI Developers.
[cix] Cloud Computing & Web Hosting | OVHcloud Worldwide; Cloud Computing & Web Hosting | OVHcloud Worldwide.
[cx] Eindrapport In het kader van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers voor het ministerie van Economische Zaken | Tweede Kamer der Staten-Generaal
[cxi] Eindrapport In het kader van het quickscan-onderzoek naar technische, organisatorische en juridische gaps tussen Europese/Nederlandse cloudproviders en Amerikaanse hyperscalers voor het ministerie van Economische Zaken | Tweede Kamer der Staten-Generaal
[cxii] European Cloud Providers: What Are the Options Today? - InfoQ
[cxiii] Best Strategic Cloud Platform Services Reviews 2026 | Gartner Peer Insights
[cxiv] CMS. (n.d.). Expert Guide on Real Estate Data Centre Consenting. CMS Law.
[cxv] (2024). European data center overview 2024
[cxvi] European Real Estate Market Outlook 2026
[cxvii] The Real Estate Power Play Behind Europe's Data Center Growth
[cxviii] See McKinsey: Unlocking the European AI revolution | McKinsey; IEA: Energy demand from AI – Energy and AI – Analysis - IEA; The Shift Project: Environmental-impacts-of-digital-technology-5-year-trends-and-5G-governance_March2021.pdf; Ember: Grids for data centres: ambitious grid planning can win Europe's AI race
[cxix] IDC Report Reveals AI-Driven Growth in Datacenter Energy Consumption, Predicts Surge in Datacenter Facility Spending Amid Rising Electricity Costs. See also: CERRE_Report_DCs_FinalPDF.pdf pp 13-15.
[cxx] For example in Dublin: Data Centres in Ireland, and in Amsterdam: Challenges in the Dutch Data Center Market.
[cxxi] Grids for data centres: ambitious grid planning can win Europe's AI race; Ember, 2025; Reuters, 2025; BCG, 2025; Power connection requests for Italy data centres rise to 42 GW at end-March | Reuters; See also: Single Market - Compendium of obstacles - 21 May 2025
[cxxii] Why Retrofit Could Dominate Data Centre Builds This Decade | Data Centre Magazine
[cxxiii] Data centre developers explore linking up to UK gas pipelines

[cxxiv] Europe primed for data centre ABS financing as investment soars | News | About Us | Linklaters
[cxxv] Why data center finance is diversifying
[cxxvi] AI Drives Cloud Player Capex Amid Cautious Overall Spend
[cxxvii] Knight Frank: Global Data Centres Report
[cxxviii] China invests $6.1 billion in computing data center project, official says | Reuters
[cxxix] North America Data Center Report Midyear 2025
[cxxx] Circular water solutions key to sustainable data centres | World Economic Forum; Mytton, D. Data centre water consumption. npj Clean Water 4, 11 (2021). Data centre water consumption.
[cxxxi] See for example Revealed: Big tech's new datacentres will take water from the world's driest areas. Globally, however, total data centre water use is much smaller than that of other sectors. See: icef.go.jp/wp-content/themes/icef_new/pdf/roadmap/icef2025_roadmap.pdf.
[cxxxii] See for example: ECIPE | The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities: The Case for a New Approach to Cloud Policy
[cxxxiii] Eurostack | Deploying the Eurostack: What's needed now.
[cxxxiv] Sovereign Cloud Technologies – EU-Lisa technology brief – June 2025
[cxxxv] Concession from the Department for digital transformation to the Polo Strategico Nazionale
[cxxxvi] Germany launches government cloud – Press release
[cxxxvii] CISPE's Buying Cloud Services in the Public Sector provides a comprehensive overview of public procurement difficulties
[cxxxviii] ECIPE, Occasional paper No. 04/2025: 'Boosting Efficiency and Quality in EU Public Services: The Need for a European Multi Cloud-First Strategy': ECI_OccasionalPaper_04-2025_LY04.pdf
[cxxxix] V-ICT-OR delivers innovative Flemish government services with Azure Container Apps | Microsoft Customer Stories
[cxl] Digitale Abhängigkeit von Microsoft: Risiken und Auswirkungen auf die EU-Wirtschaft
[cxli] "We're done" - major government organization slams Microsoft Teams as it drops Windows for good; Danish government agency to ditch Microsoft software in push for digital independence; Denmark's Digital Declaration of Independence: A Growing European Revolt Against Big Tech Dependency.
[cxlii] What is the Log4j vulnerability?
[cxliii] "EDLER, J. "Technology sovereignty for the EU: Needs, concepts, pitfalls and ways forward". Available at European Commission
[cxliv] AWS European Sovereign Cloud
[cxlv] EU Sovereign Cloud | Oracle Europe
[cxlvi] Capgemini and Orange are pleased to announce the launch of commercial activities of Bleu, their future "cloud de confiance" platform - Newsroom Orange Group
[cxlvii] Clarence | Le premier cloud souverain déconnecté en Europe
[cxlviii] Sovereign AI | Oracle Europe
[cxlix] The next chapter for UK sovereign AI | OpenAI
[cl] See for example: Die souveräne Cloud für den öffentlichen Sektor - STACKIT or Sovereign Cloud for Tech Innovation | Scaleway.
[cli] Sovereign Cloud in the EU: Providers, Challenges, and Opportunities
[clii] Introducing the Overview of the AWS European Sovereign Cloud whitepaper | AWS Security Blog
[cliii] 6G Infrastructures for Edge AI: An Analytical Perspective
[cliv] When AI Takes Time to Think: Implications of Test-Time Compute
[clv] This is a challenge already observed in the United States, where electricity prices have risen in regions with high data-centre concentration. It highlights the need for the EU to ensure a more balanced distribution of data-centre deployment across Member States, in order to prevent similar electricity price spikes in specific areas. Additional information available here: How AI Data Centers Are Sending Your Power Bill Soaring; $64 billion of data center projects have been blocked or delayed amid local opposition — Data Center Watch
[clvi] Global Data Center Trends 2025?
[clvii] Time to place our bets: Europe's AI opportunity?
[clviii] Europe Public Cloud Market Size & Outlook, 2023-2030.
[clix] Artificial Intelligence Index Report 2025
[clx] Technopolis Group et al. (2025), "Study: Cloud and AI".
[clxi] IEA (2025). Energy and AI, pp. 93-96. Available at: https://www.iea.org/reports/energy-and-ai
[clxii] Technopolis Group et al. (2025), "Study: Cloud and AI".

[clxiii] European Commission
[clxiv] ACTON, M., BOOTH, J. and PACI, D., 2025 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/9449356, JRC141521.
[clxv] Technopolis Group et al. (2025), "Study: Cloud and AI".
[clxvi] Blind, K. et al. (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. European Commission. Available at: Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy
[clxvii] See Special report 12/2025 - The EU's strategy for microchips ; Competition in artificial intelligence infrastructure (EN) and Report_Emerging-Resilience-in-the-Semiconductor-Supply-Chain.pdf
[clxviii] Technopolis Group et al. (2025), "Study: Cloud and AI".
[clxix] As mentioned in the Copenhagen Economics Study (Available here), the data centre sector can contribute to increasing FDI by fostering clusters along parts of the digital infrastructure value chain which can, in turn, attract other businesses, e.g. suppliers or technology firms benefitting from proximity to the facilities. Other factors contributing to the selection of data centre locations are also presented here: 2025-Data-Center-Site-Selection-Dynamic-Brief.pdf
[clxx] The EU attracted the most FDI projects among world's regions according to figures from fDi Markets. Data centre investors announced several mega projects, i.e. with over $1bn in committed CapEx across Europe and FDI worth more than $69bn in 2024. Figures available here: fDi's European Cities and Regions of the Future 2025
[clxxi] OECD (2025), "Competition in the provision of cloud computing services", *OECD Roundtables on Competition Policy Papers*, No. 323, OECD Publishing, Paris, https://doi.org/10.1787/595859c5-en.
[clxxii] British International Investment insight, How-does-access-to-a-local-data-centre-affect-business-productivity.pdf
[clxxiii] AWS services recover after daylong outage hits major sites
[clxxiv] WEF_Global_Cybersecurity_Outlook_2025.pdf and CrowdStrike outage: We finally know what caused it - and how much it cost | CNN Business
[clxxv] Accelerating Europe's AI adoption: The role of sovereign AI
[clxxvi] Right Scaling for Right Pricing: A Case Study on Total Cost of Ownership Measurement for Cloud Migration | Springer Nature Link
[clxxvii] Artificial intelligence: Europe needs to start dreaming again
[clxxviii] See Digitalisation and Employment, International Labour Organization, 2022
[clxxix] Findings of an unpublished Research briefing by FGS Research made available to the Commission in November 2025 (survey of 3,022 adults across 6 markets - UK, US, Japan, France, Germany, Italy – with a sub-set of questions specific to France, Germany and Italy only) indicates that (1) 71% of surveyed populations think that "Technological sovereignty helps create and protect local jobs" as opposed to 22% who insisted that Technological sovereignty harms and threatens local jobs.
[clxxx] See Infrastructure or Intrusion? Europe's Conflicted Data Center Expansion
[clxxxi] See Eurostat (2024, 2025), E-government activities of individuals via websites, Individuals - frequency of internet use and Meetings via the internet by size class of enterprise
[clxxxii] OpenAI reports that Chatgpt search alone has 120 milion average monthly users in the EU.
[clxxxiii] Ibid (1) on average, 65% of citizens in France, Germany and Italy insist that "It is worth investing more to keep technologies like satellites, cloud services, and AI systems under national control, even if that means costs are higher", as opposed to the average of 28% thinking that "It is more important to keep costs low, even if that means relying on foreign companies for things like satellites, cloud services, and AI systems". (2) On average, 54% of citizens think "Governments should lead and invest heavily in technology development to secure sovereignty", whereas 36% that "The private sector should drive technology innovation with minimal government intervention". (3) But only 39% think "It is worth spending more on developing our own technologies, even if that means less funding for other areas like healthcare", while 55% argue that "Public money should prioritise essential services like healthcare and education, even if that means relying on foreign technology".
[clxxxiv] This is in line with past expectations and figures. EEA's indicator shows that the GHG intensity of power generation in the EU has been falling for decades and was about 40% lower in 2024 than ten years before. See here: Greenhouse gas emission intensity of electricity generation in Europe | Indicators | European Environment Agency (EEA)
[clxxxv] The IEA 4E EDNA policy work underlines that reducing infrastructure use (PUE) can be achieved by smaller data centres through grants or technical support, separate from Minimum Energy Performance Standards or

obligations which may be challenging to apply to smaller data centres. Available here: Policy development on energy efficiency of data centres draft final report v1.05. Smaller operators typically lag behind hyperscalers as they lack the capital and human resource capacity to invest in efficiency innovations, leading to structurally higher PUEs, and often depending on available technologies.

[clxxxvi] https://www.networkworld.com/article/972407/5-ways-to-boost-server-efficiency.html

[clxxxvii] See also: AI, data, and computing: shaping infrastructures for a decarbonised world - The Shift Project IL

[clxxxviii] IEA (2025). Overcoming energy constraints is key to delivering on Europe's data centre goals. Available at: https://www.iea.org/commentaries/overcoming-energy-constraints-is-key-to-delivering-on-europe-s-data-centre-goals

[clxxxix] IEA (2025). Energy and AI. Available at: https://www.iea.org/reports/energy-and-ai

[cxc] European Environment Agency (2024). Water abstraction by economic sector in the 27 EU Member States, 2000-2022. Available at: https://www.eea.europa.eu/en/analysis/indicators/water-abstraction-by-source-and/water-abstraction-by-economic

[cxci] Circular thinking for data centres - Arup

[cxcii] Alissa H., Nick T., Raniwala A. *et al.*, *Using life cycle assessment to drive innovation for sustainable cool clouds*, Nature, Vol. 641, 2025, pp. 331–338, available at: Using life cycle assessment to drive innovation for sustainable cool clouds | Nature

[cxciii] Schneider Electric. (2023). Quantifying Data Center Scope 3 GHG Emissions to Prioritize Reduction Efforts—White Paper 99. https://www.se.com/ww/en/download/document/SPD_WP99_EN/

[cxciv] Swedish audit reports (2022). See: Central government initiatives to stimulate investments in data centres (RiR 2022:18)