EUROPEAN
COMMISSION

Brussels, 3.6.2026
SWD(2026) 502 final

PART 2/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the

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}

Contents

0. 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
ESO(s)	European Standardisation Organisation(s)
EU	European Union

Term or acronym	Meaning or definition
FLAPD	Refers to the data centre markets located in Frankfurt, London, Amsterdam, Paris and Dublin.
FTE	Full Time Employee
GDPR	General Data Protection Regulation
Hyperscaler	Hyperscalers are very large cloud 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.
PC	Public Consultation
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.

ANNEX 1: PROCEDURAL INFORMATION

1. LEAD DG, DECIDE PLANNING & CWP REFERENCES

The lead DG is Directorate-General for Communications Networks, Content and Technology (DG CNECT), UNIT E2: Cloud and Software.

The DECIDE reference number of this initiative is PLAN/2025/815.

The Commission work programme for 2025 includes a legislative action for a cloud and AI Development Act, under the header "3.1 A new plan for Europe's sustainable prosperity and competitiveness".

2. ORGANISATION AND TIMING

The impact assessment started in 2025, with the public consultation and call for evidence published on 9 April 2025[1].

The impact assessment on a possible cloud and AI Development Act was coordinated by an Interservice Coordination Group (ISCG). The Commissions Services participating in the ISCG were: Secretariat-General, Legal Service, DG Communications Networks, Content and Technology, DG for Internal Market, Industry, Entrepreneurship and SMEs, DG for Energy, DG for Trade, DG for Digital Services, DG for Environment, DG for Climate Action, and DG for Competition.

The ISCG met on 24 July 2025, on 12 September 2025, 28 November 2025, and 25 January 2026. It was consulted throughout the different steps of the impact assessment process, notably on all stakeholder consultation materials and deliverables from the external contractor and on the draft impact assessment before submission to the Regulatory Scrutiny Board (RSB).

3. CONSULTATION OF THE RSB

This version was submitted to the RSB on 30 April 2026. The RSB issued a positive opinion with comments on 8 May 2026. The comments received from the Board have been addressed in the revised version of the impact assessment as detailed below.

Table 1. Modifications of the impact assessment report in response to RSB comments

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
(B) Key issues		
The report should sufficiently describe the policy measure establishing a set of non-price award criteria and the one encouraging the use, reuse, development and sharing of open-source assets by the public sector.	PM16 and PM19 have been reformulated to support EU added value. The non-award criteria defined under these PMs 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	Main report sections 5.1.1 and 5.1.2 and Annex 4.

[1] AI Continent – new cloud and AI development act.

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
	additional points to tenderers. Furthermore, the criteria have been updated. Given that the costs and benefits entailed majorly administrative costs (e.g. updates of templates) these values remain unchanged. The description of PM20 in section 5.1.2 has been updated to make more explicit what it is intended with 'use, reuse, and share' in this context, arguing on the motivation to follow such an approach.	
The internal coherence between the policy measures addressing sovereign cloud and AI services and those addressing critical dependencies and supporting the use of Open Source should be sufficiently explained and assessed.	Under section 7.2. the coherence between sovereign cloud and AI services, critical dependencies and open source interplay with each other and are mutually reinforcing each other.	Main report section 7.2
The costs related to migration and porting and the related uncertainties should be sufficiently reflected in the assessment of the total costs in the main report.	A portion of the costs of porting applications have been included as part of the cost – benefit analysis. The text argues that the central value of EUR 86.3 bn should be considered as a maximalist approach, where all out of the 30% of the cloudified solutions requiring sovereign level 2, 3, and 4 of the 6 400 essential entities under NIS2 would be ported to a sovereign cloud service as of result of the intervention. A more plausible scenario has been considered, where all applications at level 4 (1% of the total applications) and half of the applications at level 3 (5% compared to the estimated 9%) will be ported over 3 years as a result of the intervention.	Main report 6.1.2, 7.2 and Annex 12, section 12.4
(C) What to improve		
The policy measures aimed at reducing critical dependencies (PM16/PM19) should be better described, in particular why the criterion "outside of the country of dependencies" is used rather than "within the EU", on the basis of which criteria the dependency threshold is set at 50%, how the non-price award criteria are to be used by public buyers, how they will be used and assessed. The report should also better discuss the representativeness of the assumptions in PM15 regarding what percentages of use cases would respectively require sovereignty levels 1, 2, 3 and 4.	PM16 and PM19 have been reformulated to support EU added value. The non-award criteria defined under these PMs 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. Under PM15, both in the main report and Annex 4, a clarifying sentence has been included to argue on the representativeness of the assumptions.	Main report 5.1.1 and 5.1.2 and Annex 4.

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
Policy measure PM20 encourages the use of Open Source in the public sector and requires the contracting authorities to assess the equivalence/superiority of Open Source over proprietary solutions in the tendering procedure. PM22 encourages EU level joint public procurement. Building on the annex, the report should better analyse the impact of these measures on public authorities, including the need for specialised expertise and interplay with envisaged Open-Source Programme Offices, as well as how a uniform approach across the EU will be ensured. The impact of these measures on the companies offering the relevant IT services should also be discussed	The description of PM20 in Annex 4 has been expanded. It is discussed that the initial administrative costs incurred due to the comparative assessment of solutions (proprietary vs. open source) in staff training would result in capability benefits in the long term. Furthermore, public authorities may rely on OSPOs as centres of excellence in open source, at technical, legal, procedural and strategic level, who can support public authorities with standardised evaluation frameworks and methodologies. Uniformity may be achieved by means of recommendations and experience sharing in the OSPO networks. The new text also includes how these new conditions would impact businesses, both providers of proprietary solutions and open source solutions, and the overall market.	Annex 4, description of PM20; main report section 6.1.2 and 6.1.4
Regarding external coherence: as the policy measure PM11, defining the sovereignty levels and the associated requirements, includes criteria based on the European Cybersecurity Certification Scheme for Cloud Services (EUCS), which has not yet been adopted, the report should describe in more detail the interplay of the two initiatives as well as implementation uncertainties for EUCS	PM11 includes the inter-relation between the sovereignty levels and EUCS as one of the criteria to fulfil. This footnote argues that 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 an enter into force in early 2029. EUCS technical work is done 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 to be adopted under the Cybersecurity Act, a process much shorter than CADA's interinstitutional negotiations.	Main report 5.2.2 and Annex 4, as a footnote in PM11.
In view of the impact on the total costs of the initiative, the costs related to migration and porting, described in box 2 and in the annex, should be reflected in a summary table of costs and benefits.	The table and text in section 7.2 have been modified to reflect the costs of porting. Under 6.1.2 the estimated costs are detailed based on the explanations provided under Annex 12, section 12.4, which has also been updated.	Main report 6.1.2, 7.2 and Annex 12, section 12.4

Table 1. Modifications of the impact assessment report in response to RSB comments

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
(B) Key issues		
(1) The key proposed policy measures are not sufficiently specified to allow for the assessment of those measures and whether they can address the identified problems of EU competitiveness and strategic autonomy. Their proportionality is not adequately demonstrated.	In response to the Board's comments regarding the measures designed to respond to Problem 2 and its corresponding drivers, the updated impact assessment proposes a more refined and proportionate approach to how sovereignty would be defined in CADA and how it would be practically implemented by public administrations. PM11 now defines sovereignty along four levels (instead of one level, which required exemptions for particular cases), of which higher levels come with higher sovereignty demands. This allows for greater granularity in answering customers' needs and reflects with more nuance the reality of available and future service offerings. The layered approach reinforces the proportionality of the measure. It aligns better with the available offer from European operators. It increases trust and enables broader cloudification of on-premises solutions of the most critical use cases, while creating new market opportunities for sovereign European providers. PM11 now also includes a dedicated synthesis table providing a consolidated view of the gradually demanding sovereignty criteria. The assessment of conformity against the respective sovereignty levels is also more balanced and cost-effective for all parties involved, notably in terms of administrative burden on public authorities. As introduced by PM15, compliance against sovereignty level 1 would be based on self-assessments conducted by the service provider. 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 (a mechanism similar to that used in the Digital Services Act). We make it explicit that services from non-European providers can qualify for Level 1 and Level 2, but not for Level 3 and Level 4. The measure remains anchored in addressing the protection of public order in the public sector (SO4). But since the new Level 3 and Level 4 are reserved to EU providers (on sovereignty grounds), it nevertheless justifies that this measure also addresses the overall dependence	Main report: section 5.2.2. (and all subsequent analytical sections)

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
	on non-European cloud and AI computing services (SO3). The sovereignty risk assessment newly introduced by PM15 allows Member States to identify which public sector use cases within require the use of which sovereignty level. This approach reinforces the subsidiarity dimension of the measure. It empowers Member Stats to integrate sovereignty criteria in their established practices and to better choose or change providers where the sovereignty risk assessment has determined so. It limits transition costs, by allowing Member States to consider their own budgets so that the transition to sovereign solutions naturally follows their existing investment schedules. Finally, it avoids big one-off expenditures by public authorities and diffuses any risk of a supply crunch since the uptake of sovereign services will be more gradual. In this context, to ensure methodological clarity and appropriate degree of delineation between the different measures analysed, the previous PM19, part of PO2-B, which consisted in sovereignty audits to be conducted in the public sector has been removed altogether as it was too close of the sovereignty risk assessments now conducted under PM15 and PM21. A new PM19, now part of PO2-C, has been spun off from PM21 and consists in the award criteria made mandatory.	
(2) The analysis of effectiveness and efficiency does not adequately reflect all the costs (i.e. transition costs). The benefits appear to be over-estimated.	The updated approach to sovereignty is reflected in the way costs and cost savings are calculated. Based on the feedback of the Board, the impact assessment now includes in the costs not only those corresponding to the establishment of the measures, but also transition costs directly in the calculations, and not at a macro-economic level. In response to the Board's targeted comments and based on new evidence, the impact assessment introduces an improved sensitivity analysis of the effective price mark-up of sovereign solutions, as described in *section 2.3.4*. This results into a more robust range-based calculation of impacts across the applicable PMs detailed in *Annex 4, section 3*. We now also analyse the costs for a customer to port individual IT systems from one provider to	Main report: section 2.3.4., 6.1.2., 6.1.5 Annexes: Annex 4, section 3. Annex 12

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
	another. This is summarised in a new box under *section 6.1.2* and detailed in the new *Annex 12* provides which also covers the case of migration (cloudification) of legacy applications. It includes the migration/switching journey broken down into distinct phases and accounts for three gradual application sizes for which the corresponding costs are calculated. In response to the Board's comments regarding the previous approach to quantification of benefits, *section 6.1.5.* now provides a more narrowly defined and qualitative analysis of macro-economic effects. The first part of the new qualitative analysis focuses on benefits for public administrations related to improved sovereignty stemming from the use of sovereign services, lesser dependency on 3rd-country providers. The second part provides a qualitative analysis of the commercial spillover in terms of improved market opportunities for providers serving use cases associated with Level 3 and Level 4, related for example to improved visibility and perception in terms of service quality from the perspective of private buyers.	
(3) The analysis of coherence must be reinforced as there are apparent overlaps with existing and upcoming legislation.	*This comment is addressed under the more detailed point 4 of the What to improve section.*	
(C) What to improve		
(1) Given the market situation and the stated specific objectives, the interplay between the criteria for authorising sovereign cloud services and existing legislation in third countries should be clarified and the resulting impacts analysed. The report must provide a robust estimate of the number of entities affected by mandatory requirements regarding sovereign solutions, as well as which sovereign cloud services EU service providers currently do not offer. The report should explain how "countries with dependencies" will be identified as well as how and by whom the criterion of equivalence/superiority will be established for the prioritisation of open source. Without these	The updated *PM11* provides under *section 5.2.2.* a granular description of the four levels of sovereignty, including a breakdown of the gradually demanding requirements. *PM11* now also includes clarifications as to which types of providers could qualify for which sovereignty level, all in view of the increasing level of assurance provided between Levels 1 and 4 against the risks defined under Problem 2. New analysis provided under *PM15* in *Annex 3, section 3.15.* connects the new stratified approach to sovereignty with current market realities with regard to providers in scope of CADA. The section details the number and type of providers who could reach the respective levels of sovereignty. We assess that 59 non-EU headquartered providers meet Level 1 requirements and would be able to qualify to Level 1 or 2 should they decide so. 226 EU headquartered providers could qualify as Level 1 or 2 and would be able to qualify as Level 3	Main report: section 5.2.2. (and all subsequent analytical sections), section 6.1.2., section 2.3.2. Annexes: Annex 3, section 3.1.5., section 3.2.1. Annex 12, Annex 13

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
clarifications the impact and proportionality of the intervention in terms of costs, including transition costs, and benefits cannot be credibly assessed.	should they decide so. Some of these providers are large companies with proven track record already in serving governments. We also clarify that at this moment, few European providers can achieve Level 4 but more are expected to reach this level soon. When it comes to the requested strengthened analysis of the number of entities impacted by the obligations under *PM21*, section 6.1.2. includes real life evidence-based calculations of costs of porting applications between two cloud environments with a view for three distinct types of public authorities (small, medium, high) and the implied IT system complexity. *Annex 3, section 3.21*. 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 all 6400 public entities possibly in scope is presented under the new *Annex 12*. The new *Annex 13* provides a comparative analysis between offerings of the three leading hyperscalers and three selected European providers. Complementing the previous description of the difference in terms of the number of offerings under *PD1, section 2.3.2.*, the Annex provides a much more granular and nuanced assessment of this. A set of dedicated tables shows that the selected European providers already offer services broadly equivalent to those of AWS, Microsoft Azure, and Google Cloud Platform across the core infrastructure categories that are most widely used: compute, storage, network, and managed container orchestration. The comparison has been extended to office automation suites, one of the most widely adopted SaaS categories in the public sector, where credible European and open-source alternatives are also available. Where previous interviews have shown that most public administrations use an average of twenty services, instead of the whole range offered by hyperscalers, the Annex demonstrates that EU providers already offer the most used services and with a similar level of functionality. With respect to the identification of countries of dependence, *PM16*, under *section 5.2.2.* now details the methodology to establish the	

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
	necessary degree of dependence as well as the necessary evidence collection and notification to Member States contracting authorities. Finally, regarding the approach to establishing equivalence or superiority of an open source solution to define its priority over a proprietary one, *PM20*, under *section 5.2.2.* now provides further operational details related to this assessment.	
(2) The analysis of benefits must be based on robust and verifiable assumptions and methodologies. Although the report acknowledges the arbitrary choice of certain assumptions and parameters used for assessing the impact of key measures under the preferred option, those (for example increased market shares, risk parameters allocation between the various options, mark-up percentage for sovereignty increased costs) appear to drive the results of the analysis.	In response to this comment, the modelling has been reviewed for all PMs where changes were implemented. Where appropriate, to ensure the most convincing analysis attainable, we have shifted from a quantitative to a qualitative assessment, including with respect to increased market share of European providers (as explained in response to the Key issue #2). The analysis of a price mark-up for sovereign solutions and the sensitivity analysis thereof has also been redone and is now based on newly available empirical evidence, as detailed in *section 2.3.4.*	Main report: Section 2.3.4., 6.1.5.
(3) The report must provide a more comprehensive analysis of technical, functional and operational consequences of key measures (i.e. PM 20, 21). As certain measures (in particular PM 21, embedding PM 11, 15 and 16) aim at building an EU sovereign cloud, the impacts of the limitations of supply from third countries must be assessed, including the time and costs estimated for EU service-providers to offer equivalent substitutes. The report should assess the pass-through of these cost	As part of the assessment of economic impact on industry, including SMEs and private sector essential entities, *section 6.1.1.* now includes a dedicated Focus box detailing in qualitative terms (with several illustrative pieces of quantitative evidence) the costs for service providers to develop sovereign services or raise the conformity level of existing services. This section should be read in conjunction with the new Annex 13 providing a comparative analysis between offerings of the three leading hyperscalers and three selected European providers.	Main report: section 6.1.1. Annexes: Annex 13
(4) The report should provide a detailed analysis of coherence, in particular of the authorisation scheme for cloud and AI computing services with the security risk assessment in the Cybersecurity Act and of public procurement measures with the upcoming revision of the public procurement rules. This should be accompanied by	*Section 7.3.* now includes a detailed description of delineation and complementarity between CADA and the Cybersecurity Act 2 (CSA 2) on one hand and the upcoming Public Procurement Act on the other. With regard to the CSA 2, this section details the complementarity between the cybersecurity measures established by the Act and the sovereignty criteria put forward by CADA. The risk assessments introduced by the CSA 2 and the possible prohibitions and other mitigating	Main report: Section 7.3 Annex 7

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
an analysis of the potential additional legal complexity and administrative burden.	measure, including with respect to high-risk vendors, provides a cybersecurity baseline which CADA builds over by introducing a targeted approach to mitigating sovereignty risks specific to the provision and use of cloud and AI computing services. Similarly, the gradual sovereignty levels established by PM11, PM15, PM21 incorporate increasingly demanding compliance against the three assurance levels of the future European cybersecurity certification scheme (EUCS). The section also explains the absence of any overlap between the requirements of the CADA sovereignty levels and the applicable requirements and those assessed under the EUCS, which exclusively covers technical cybersecurity aspects. Finally, *PM21* details further how private sector essential entities listed under Annex I of NIS 2 will have 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. Accordingly, *section 6.1.1.* clarifies the costs of such entities integrating sovereignty considerations in their existing risk assessment activities. With respect to applicable legal framework of the Public Procurement Directives, currently under review, all measures of CADA related to public procurement are compatible with the rules in place and those anticipated to be proposed by the Commission under the new framework. Notably the measures related to restricted access to public procurement under *PM15* and *PM21* incorporate the justifications necessary to comply with the requirements of the exemptions foreseen in the Government Procurement Agreement of the World Trade Organisation. Additionally, based on targeted consultation with DG GROW, the section now details the interplay between horizontal measures related to admissible means of incorporating "EU preference" requirements in public procurement which the Public Procurement Act should provide and the sector-specific approach leveraging award criteria under PM16 and PM19 of CADA.	

Table 2. Modifications of the previous version of the impact assessment report in response to RSB first negative opinion

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
(B) Key issues		
(1) The key proposed policy measures are not sufficiently specified to allow for the assessment of those measures and whether they can address the identified problems of EU competitiveness and strategic autonomy. Their proportionality is not adequately demonstrated.	A clearer description of the market historical context and evolution has been added before introducing the problems of the intervention. Moreover, problem drivers 1 - 4 have been updated to better reflect relevant failures and the regulatory complexity at play.	Main report: section 2.1, section 2.2, section 2.3
(2) The aspects of EU strategic autonomy are insufficiently reflected in the report.	The general objective, and the specific objectives 3 and 4 have been updated to include a clearer strategic autonomy dimension.	Main report: section 4
(3) The proposed policy measures, including on EU 'sovereign' solutions, are not clearly defined and the causal links in the intervention logic are not sufficiently substantiated.	The description of the policy measures has been improved both in section 5.2 and in annex 4, notably PM11, PM15 and PM21. The causal links have been included also in section 5.2. Furthermore, the table in section 5.2.3 has been updated to show clearer the link between the problem drivers, the problems, the policy options, policy measures and specific objectives. Finally, a new table has been added in section 5.2.4 to better demonstrate which aspects of each problem driver the proposed policy measure address.	Main report: section 5.2 (notably 5.2.1, 5.2.2, 5.2.3 and 5.24)
(4) The analysis of effectiveness and efficiency does not sufficiently reflect the adjustment costs, technical feasibility and unintended consequences linked to the proposed policy measures.	Adjustment and administrative costs have been cross-checked and updated in the main report under section 6 and Annex 4. While quantitative estimates of all possible adjustment costs and unintended consequences were at times limited by data availability, the effectiveness and efficiency analysis have been revised and the discussion to address transition costs, technical feasibility and possible side effects of the proposed measures, expanded. This has been added under section 7.1 and 7.2. The sensitivity analysis in section 7.5 has also been updated to clearly present the uncertainties linked to the proposed policy measures.	Main report: section 7.1, 7.2, 7.5 Annex 4
(C) What to improve		
1) The report should better analyse the root causes of the insufficient cloud capacities in the EU and the declining market share of European services providers.	Section 2.1 (Problem context) has been reformulated to include an analysis of the main drivers for the current situation of the declining market share of EU providers.	Main report: Section 2.1, Section 2.2, Section 2.3

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
Based on an analysis of the main drivers of competitiveness, such as price, scope of services, innovation and quality, including cyber security, it should analyse potential market failures. It should also analyse potential regulatory failures based on available evidence of investment decisions. It should analyse more thoroughly the current practices and regulatory frameworks in Member States and how they impact the Internal Market. It should describe the risks of reliance on non-EU providers and the potential trade-offs with aspects of strategic autonomy.	Problem drivers 1-4 have been updated to showcase better the different failures, such as market and regulatory related ones. Problem driver 1 has been updated seeking to respond to the aspects related to the main drivers of competitiveness. Problem driver 2 has also been updated and reformulated to better substantiate the fragmentation of the different regulatory frameworks across MS. Problem driver 3 has been updated to discuss the risks of reliance to non-EU providers, notably for the public sector.	
2) The report should be clear whether – and if yes how - the objectives of this initiative relate to the EU's strategic autonomy. What level of autonomy is to be achieved and in which domains? The content of policy measures should be clearly defined, including the criteria for "sovereign solutions" and "EU-made". The report should better justify how the target of market share of EU providers is set.	The general objective as well as specific objectives 3 and 4 have been updated to include a clearer strategic autonomy dimension. The explanations of the main elements of the policy measures have been updated in section 5.2. Further explanations and details have been included in annex 4 under each PM11, PM15, PM16 and PM21 to clarify this. Section 6.1.5 has been updated to include a justification of how the increase of market share from 15% to 30% has been used and what has been the rationale for such an assumption. A new section has been included in Annex 4 (section 8.3) aiming to better explain the feasibility of the move towards a market share of 30% by EU providers per customer segment.	Main report: Section 4, Section 5.2, section 6.14 Annex 4 section 7.2, section 3 and section 8.3
3) The report should assess the potential impacts related to the criteria for "sovereign solutions". It should analyse in sufficient detail the levels of sovereignty to be reached and be transparent about technical prerequisites needed. The report should assess all the adjustment costs and quantify them to the extent possible and be clear on who will bear these costs. The report should provide a more comprehensive analysis of unintended consequences, including on cyber security, in particular related to	The report has been modified in section 5.2 and annex 4, where a clearer definition of the sovereignty criteria is provided. Annex 4 and section 6.1 have been amended to clarify which adjustment cots have been considered for the sovereignty aspects. Additional explanations and justifications have been included to motivate the rationale of why certain adjustment costs have not been considered. The sovereignty criteria that have been discussed in the report will result in a unique level of sovereignty. However, the report has been edited to include the notion of "sovereignty-readiness" in section 5.2 and	Main report: section 5.2, section 6.1, section 2.2.3. Annex 4 section 3, description of PM11, PM15 and PM21

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
sovereignty and open-source requirements.	annex 4, to clarify that not all cloud and AI computing service providers will start from the same situation and what this may entail. The unintended consequences of cybersecurity and open source have been described in PD3, which has been adjusted accordingly.	
4) The analysis of benefits should be based on robust assumptions, in particular for PO2B and PO2C where stated benefits are very high. For example, all implications should be factored in the analysis, such as investments needed to maintain cyber security, and the scale needed to make them viable in economic terms. In terms of the environmental footprint, the report should explain the mechanisms leading small(er) EU cloud providers to significantly reduced Power Usage Effectiveness values and how European-funded R&D initiatives are expected to deliver superior results when compared to the efforts of global hyperscalers.	For PO2-B and PO2-C in annex 4 a clarification has been added both under PM15 (applicable to PO2-B) and PM21 (applicable to PO2-C) on the costs that have been included, the ones that have been excluded and the rationale behind them. The report has also been updated to include additional considerations on the environmental impact of data centre capacity, with clearer explanations of how EU-funded R&D initiatives and other Policy Measures are expected to accelerate the adoption of energy-efficient technologies within data centres and thus leading to a long-term reduction in PUE levels, compared to the other options and baseline. The timing dimension of this reduction was also further considered as programmes require time to develop and market new solutions that would optimise energy-efficiency. The report does not suggest that EU-funded R&D is expected to outperform or deliver superior results when compared to hyperscaler-led investments in innovation. Rather, the discussion focuses on how public R&D support and related policy instruments could help facilitate the diffusion and adoption of current and new technologies across the wider data centre ecosystem, and in particular among non-hyperscale operators, which have been found to exhibit higher average PUE levels than hyperscale facilities.	Main report: Section 6.3 Annex 4
5) The report should allow for verifiability of the economic modelling. It should quantify and monetise only benefits which can be clearly linked to the policy measures and whose quantification can be substantiated by evidence. Currently the benefit cost ratios presented in the report are not plausible. After revision of the analysis of costs and benefits, the sensitivity analysis should be reviewed in order to allow to assess uncertainty related to the most impactful variables behind the projections.	The cost benefit analysis has been revised. The benefits modelled in annex 4 include only those that can be quantified and monetised; however, as an additional exercise, the indirect benefits, not quantified, had already been included in the previous version of annex 4 under most policy measures. Most of the assumptions remain in line with what had been previously presented. These were validated in one-to-one interviews, CATI surveys and the final validation workshop of the study led by Technopolis. In the event of uncertainty, assumptions were discussed in the final validation workshop. Except for a couple	Main report: section 7.5 Annex 4

Opinion of the RSB by point	How comments have been addressed	Sections in IA report/Annex
	of them (authorisation effort and PUE) all other assumptions were confirmed by attendees. The explanations for the sensitivity analysis have been improved in section 7.5	
6) The coherence, complementarity and potential synergies with other initiatives - such as the Cybersecurity Act, Data Act or the public procurement revision - should be analysed in more detail.	Additional clarifications on external coherence with the Cybersecurity Act, the Data Act and the public procurement revision have been added to section 7.3, on top of the existing analysis in Annex 7.	Section 7.3 of the main report

4. EVIDENCE, SOURCES AND QUALITY

The impact assessment is based on several sources, including:

1. Stakeholder consultation activities (see Annex 2)
2. External support study carried out by an independent consultant (Technopolis Consulting Group Belgium coordinator - SPECIFIC CONTRACT No 4500075392 implementing framework contract No FW-00141707 CNECT/2022/OP/0036 - Framework Contract for the provision of Studies and related services on digital policy issues Study: cloud and AI – STUDY 2024-046)

ANNEX 2: STAKEHOLDER CONSULTATION (SYNOPSIS REPORT)

1. INTRODUCTION

This annex provides a summary of the consultation activities undertaken to gather evidence and ensure that the public interest is well reflected in the design of potential policy measures for cloud and AI computing services development within the EU. It presents the range of stakeholders consulted, describes the main consultation activities and provides an analysis of their views and the main issues they raised. The objective of the consultation activities was to collect the views and experience of stakeholders on the key problems and associated drivers related to cloud and AI infrastructures in Europe, including current and future capacity needs, sustainability, investment conditions, and the availability of secure EU-based providers and services. In addition, it aimed to gather information and their opinions on the definition of relevant policy objectives linked to those problem areas and the identification, definition and screening of policy measures that could eventually be incorporated into policy options for this impact assessment as well as gather information and opinions on their likely impacts.

2. OVERVIEW OF CONSULTATION ACTIVITIES

2.1 Public Consultation on the Cloud and AI Development Act

The Public Consultation ('PC') consisted of an online questionnaire available in English, French and German; and a Call for Evidence (CfE) for stakeholders to submit detailed position papers outlining their views and recommendations on the objectives and proposed actions envisaged by the cloud and AI Development Act, while also giving direct evidence to inform the design of policy options. The questionnaire and the Call for Evidence ran from 9 April 2025 to 3 July 2025. In addition to the OPC, the following consultation activities were conducted:

- Targeted Workshops with relevant stakeholders;
- Ad-hoc contributions and targeted consultations with Member States, small-and-medium sized enterprises (SMEs) and other relevant stakeholders;
- Targeted consultations with industry representatives and public authorities through surveys and workshops as part of a study commission by the Commission to support the impact assessment.

2.2 Study to support the impact assessment

The Commission contracted a study to a consortium led by Technopolis Group to provide empirical evidence on the currently available computing capacity across Europe and to assess present and projected future cloud computing needs within the EU. The study addresses knowledge gaps in cloud computing development and provides policy recommendations to support the Impact Assessment. The study incorporates multiple stakeholder engagement activities, including targeted interviews (over 60), surveys (with over 250 replies) and workshops (over 100 participants). The results of those activities are also included in this annex.

2.3 Overview of workshops, seminars and roundtables:

- Workshop with 70 industry actors on industry needs for cloud computing capacity for AI demand (4 October 2024, Brussels, Belgium);
- Seminar with industry, academia and public authorities on the economic dynamics of the AI stack (4 April 2025, online);
- Workshop with industry on the rationale and policy options that underpin the Act (14 May 2025, Berlin, Germany);

- Workshop with the Information Technology Industry Council (15 May 2025, Brussels, Belgium);
- Roundtable on investment in cloud compute with financial investors (20 May 2025 Brussels, Belgium);
- Presentation on future EU cloud and AI policy with industry (3 June 2025, Bilbao, Spain);
- Workshop on the preliminary findings of the accompanying study of the cloud and AI Development Act (6 June 2025, Brussels, Belgium);
- Roundtable on policy measures to facilitate data centre integration to the EU grid (18 June 2025, Brussels, Belgium);
- Roundtable with European Cloud Service Providers' CEOs on developing sovereign cloud offerings in the EU (23 June 2025, Brussels, Belgium);
- Workshop during the 6th General Assembly and Alliance Forum of the European Alliance for Industrial Data, Edge and Cloud (8 July 2025, Brussels, Belgium).
- Roundtable with American Chamber of Commerce (22 October 2025, Brussels, Belgium);
- Workshop on the final findings of the accompanying study of the cloud and AI Development Act (12 November 2025, Brussels, Belgium);

2.4 Awareness raising events in Member States and international outreach

The Commission conducted stakeholder activities across several Member States, participating in bilateral meetings with a diverse range of stakeholders in Poland, Germany, the Netherlands and Spain to discuss the problem drivers and core elements of the proposed legislation. The Commission also maintained dialogue with Member States' relevant authorities through the European Alliance for Industrial Data, Edge and Cloud ('Cloud Alliance') and bilateral meetings in Brussels. Furthermore, the Commission engaged in bilateral discussions with third countries, including Japan, Switzerland and the United Kingdom, to present and discuss the considered policy options while gathering insight on best practices.

2.5 Bilateral meetings with industry, academic institutions, think tanks

The Commission conducted over 100 bilateral meetings with a diverse array of stakeholders, including industry representatives, academic institutions, think tanks and civil society organisations to gather feedback on the design of policy options for the cloud and AI Development Act. These meetings facilitated an open dialogue with both European and international partners regarding their perspectives, concerns, and recommendations across the different policy pillars of the cloud and AI Development Act.

3. PARTICIPANTS AND METHODOLOGY

3.1 Participants

A total of 436 responses to the PC were received: 243 for the consultation survey and 193 for the Call for Evidence. The largest share came from EU citizens, accounting for 33% of all responses. This was followed by companies (28%) and associations and trade unions (18%). Additional contributions came from academic and research institutions (9%), civil society and consumer organisations (7%), and public authorities (4%). Only 2% of all respondents were non-EU citizens.

In terms of geographical origin, 90% of respondents (393) were based within the EU. The remaining 10% (43 responses) came from non-EU countries, including the US (25 responses), United Kingdom (10), Switzerland (2). The Member States with the highest participation rate were Spain (78 responses; 18%), Germany (57; 13%), and both France and Belgium (56; 10% each). No responses were received from Bulgaria, Croatia, Latvia, or Malta.

The 243 respondents to the questionnaire comprised 66 companies and private businesses (27%) including 17 SMEs, 96 EU citizens (39%), and 13 public authorities (0.4%). Out of the 66 companies and private businesses, 57% were AI developers or deployers, 56% were cloud/edge/AI users, 48% were cloud/edge/telecommunications providers, 45% were data centre operators, and 7% were financial institutions.[2]

3.2 Methodology

The responses to the OPC were subjected to quantitative and qualitative analyses. In the quantitative analysis, the respondents were ordered into the main categories considered relevant for the analysis. The answers were mapped and analysed to identify patterns as regards "who thinks what?". When considering the views of respondents on questions where they were asked to rank on a scale of 1 to 5 (1 = not very important, 5 = very important), only responses ranked 4 or 5 were considered when determining respondents' positions on each issue. The qualitative analysis of open responses and position papers was carried out in two stages. In a first step, the content of the submissions was synthesised to capture the main experiences and feedback of respondents. In a second step, these summaries were clustered according to the type of issue raised, so that contributions addressing comparable concerns were considered together irrespective of their specific wording. This approach allowed for a structured overview of the main perspectives of the respondents.

4. ANALYSIS OF THE STAKEHOLDER CONSULTATION

The respondent input gathered through the OPC highlighted four core policy challenges, which directly informed the structure of potential policy options under consideration for the cloud and AI Development Act. The main challenges and problems identified through the OPC are:

1. The strategic dependency of EU businesses and public authorities on non-EU providers of AI and cloud services, raising questions about sovereignty, resilience, and competitiveness;
2. Structural and regulatory bottlenecks hindering the expansion of data centre capacity across the EU, particularly in the face of growing AI-related demand;
3. Barriers to the digital transformation of the public sector, including limited capacity, fragmented compliance, and complex procurement procedures; and
4. The absence of a common EU-level definition and operational criteria for 'sovereign' cloud and AI computing services, leading to legal uncertainty and inconsistent implementation across Member States.

4.1 EU businesses and public authorities' dependency on non-EU cloud and AI providers

The hyperscalers are recognised for their ability to deliver comprehensive, ready-to-use business services that European providers have yet to match. For example, in terms of AI computing services, out of the respondents that provided an answer in the questionnaire, 48% indicated that only hyperscalers could offer those services and only 3% said that European providers were capable of offering those services. Despite this reliance, respondents emphasized the critical need for trusted EU-based cloud service providers, particularly for

[2] The sum of the percentages is higher than 100 as one company may be involved in more than one sector.

processing sensitive data. When selecting cloud service providers, users prioritise cybersecurity (97%), data location (87%), connectivity (81%), and innovation (81%) as their primary criteria.

Among respondents who provided an answer, when selecting a cloud provider, 82% were concerned that provider was headquartered in a third country that poses specific cybersecurity threats to the EU. In addition, 58% were concerned about vendor lock-in and 42% considered as a challenge the limited access to computational capacity in the EU. Finally, 89% considered that the location of the data was one of the main factors impacting their choice of Cloud/Edge/AI provider.

In the CfE, public authorities showed widespread concern about Europe's dependency on non-EU cloud and AI providers; however, there was some divergence on the solutions. Some authorities described the situation as a "market failure" due to the lack of viable European alternatives in key service areas and called for supplier diversification. Other public authorities advocated risk-based approaches to avoid protectionist outcomes. Some EU citizens questioned the structural reliance on private actors and proprietary systems while advocating for an EU-first approach and arguing that transformation cannot succeed while relying on foreign vendors whose strategic incentives may not align with public interest objectives.

4.1.1 Policy measures

In the CfE, respondents were generally in favour of simplifying permitting requirements and one-stop-shop to facilitate the deployment of data centres in the EU (see Section 4.2.1 below). European companies and business associations expressed strong interest in setting up sovereignty requirements and introducing "Buy EU" criteria in public tenders, whereas their global counterparts cautioned against digital protectionism and argued digital trust could be achieved without exclusion based on geographical origin (see Section 4.4.1).

4.2 Bottlenecks to expand (sustainable) data centre capacity within the EU

Data centre operators ('operators') demonstrated strong investment intentions in AI infrastructure, with 80% of them planning to expand capacity within the EU. Among operators, 77% replied future infrastructure would be dedicated to general purpose computation, 70% indicated it would be used for AI model inference, 60% on AI model training, and 33% on edge AI.

Despite this enthusiasm, operators face substantial barriers that may hamper their expansion plans. Complex and lengthy permitting procedures emerged as the primary challenge (87%), followed closely by limited access to energy resources (83%). The prevalence and severity of these obstacles is illustrated by the fact that 57% of operators need on average between 3 and 5 years for the data centre to be operational, and 13% of them need between 5 and 7 years.

The presence of those bottlenecks is supported by the responses to the CfE where connection to the electrical grid was also identified as a key bottleneck by several respondents. One business association indicated it could take up to 7 or 8 years for transmission access and two operators mentioned grid connection could take up to a decade. In addition, one business association considered those problems were exacerbated by growing local opposition to the construction of data centres, a phenomenon often termed "not in my backyard".

The factors considered by operators regarding building new data centres or expanding existing infrastructures are energy availability (91%), as well as long approval times (83%), permitting procedures (82%) and the complexity of the regulatory framework (75%).[3] Those factors reflect the importance given by operators to grid connections and the entire permitting process.

Access to finance also appears to be a common hurdle with 50% of operators and 53% of Cloud/Telco/edge providers considering high interest rates as a limitation when expending their capacity in the EU.[4] In addition, several SMEs expressed mounting concerns over high operational costs when it comes to infrastructure expansion in the EU.

In the CfE, public authorities agreed on the need for increased data centre capacity while stressing different strategic priorities. Industry associations identified fragmented permitting regimes across Europe, limited energy access, and regional disparities as persistent constraints on capacity scaling. It is important to note that in the CfE, some EU citizens challenged the expansion narrative entirely, criticizing the approach for the ignoring social and environmental costs of AI and advocating for binding limits on resource consumption rather than efficiency improvements alone.

4.1.2 Policy measures

Overall, across all respondent groups, 45% considered that having a one-stop-shop service to deal with permits at different administrative levels should be a priority action at EU level to boost the availability of sufficient and adequate cloud capacity for AI workloads; and 46% considered it essential to reduce the amount of time needed to obtain the necessary permits and environmental authorisations. Finally, 55% were in favour of creating expedited approval mechanisms and clear conditions for critical or strategic projects.

Table 2. EU policy measures on simplification of infrastructure permitting procedures

Policy Measure	Companies (SMEs)	Data Centre operators	Public Authorities	EU Citizens	Business associations/ trade unions	CSOs[5]
One stop shop service for managing permits	59% (41%)	83%	46%	43%	56%	15%
Reduce time to obtain permits and environmental authorisations	71% (53%)	93%	23%	38%	60%	21%
Expedited approval mechanisms for critical/strategic projects	79% (71%)	97%	54%	49%	57%	27%

In the CfE, several industry associations and companies recommended the creation of EU-level zoning guidelines, one-stop-shop permitting hubs, and fast-track authorisation for sustainable projects. This was echoed by investment respondents who stressed that streamlining permitting procedures would significantly enhance the sector's attractiveness for capital allocation.

In terms of sustainability, 69% of respondents supported funding for R&D of energy-efficient technologies. This was echoed in the CfE by a Member State's government which suggested R&D&I for data centre technologies enhancing sustainability, as well as several business

[3] The respondents who did not provide an answer to that question were not included to calculate the percentage of respondents.
[4] The respondents who did not provide an answer to that question were not included to calculate the percentage of respondents.
[5] The category Civil Society Organisations (CSOs) include NGOs, consumer organizations, environmental organizations, and academic/research institutions.

associations and companies. In addition, 62% were in favour of tax incentives for using sustainable technologies. In terms of EU actions that should be prioritised to boost the availability of sufficient and adequate cloud capacity for AI workloads, 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.

Table 3. EU policy measures to address sustainability aspects of data centres

Policy measure	Companies[6]	DC operators	Public authorities	EU citizens	Business associations / trade unions	CSOs[7]
Clear environmental compliance requirements	64%	73%	46%	86%	60%	70%
Addressing energy availability	73%	80%	54%	77%	50%	61%
Addressing land availability	47%	47%	23%	65%	47%	52%
Funding for research and development of energy-efficient technologies	61%	57%	54%	83%	60%	58%
Tax incentives for using sustainable technologies	70%	73%	54%	67%	60%	39%

In the CfE, multiple business associations and companies suggested the introduction of targeted tax incentives to build sustainable and energy efficient cloud infrastructure. Some considered this would be more useful than duplicating the current environmental regulations. One company suggested to create tax incentives for data centre operators that implement sustainable technologies, including waste heat reuse or immersion cooling. In addition, one business association was in favour of public-private partnerships to build sustainable, innovative cloud infrastructure. Some public authorities recommended strategic infrastructure funding to be tied to interoperability and climate goals.

Overall, this shows a strong support by different respondent groups to address existing bottlenecks in the deployment of data centres and to ensure those are sustainable and energy efficient.

4.3 Barriers to public sector transformation and public procurement

Cloud adoption in the public sector is already widespread with 85% of respondents (i.e. public authorities) storing data in cloud environments. This data often includes sensitive information (46%), commercially sensitive material (38%), or content related to public security and health (23%). The sensitive nature of this data creates heightened concerns about exposure to third-country authorities and the cybersecurity risks associated with cloud service providers headquartered in certain jurisdictions.

Such a problem is not theoretical as 69% of public authorities acknowledged that their procured providers were subject to non-EU jurisdictions including laws with extraterritorial effect. In addition, 77% of public authorities cited security risks as one of the primary obstacles preventing broader public sector cloud adoption, alongside regulatory barriers, including

[6] In each policy measure, companies include data centre operators, cloud/edge/telecommunications providers, cloud/edge/AI users, AI developers and AI deployers, and financial institutions.
[7] The category Civil Society Organisations (CSOs) include NGOs, consumer organizations, environmental organizations, and academic/research institutions.

procurement requirements (68%), and insufficient technical capacity to assess and procure appropriate cloud services (62%). In addition, 62% of public authorities mentioned fear of vendor lock as a challenge in the adoption of cloud.

These concerns are echoed by EU citizens since 76% considered public services in the EU should not be allowed to store citizen data with non-EU cloud providers, only 9% considered it depended on the type of service or data.

In the CfE, regional and local authorities identified administrative barriers such as fragmented national audits, inconsistent certification requirements, and burdensome permitting processes as core obstacles. Overall, multiple respondents emphasized that underlying market structure issues such as vendor lock-in and limited portability represent real barriers.

4.1.3 Policy measures

To address these barriers, public authorities advocated for coordinated EU-level action, with 84% supporting the establishment of cybersecurity guidelines, 77% supporting the adoption of standards, open specifications, and mechanisms to ensure interoperability. Finally, 77% advocated for a mechanism to allow federation of cloud services across public administration within and across Member States. In terms of policy actions to address the current problems faced by public administrations regarding procurement, 85% of public authorities support the creation of guidelines with standard criteria to procure cloud services and 69% support guidelines with standard award criteria. Regarding cloud and AI computing services more generally, 61% would support the creation of a marketplace for cloud and AI computing services.

In addition, overall, 74% of respondents support an open source software ecosystem. The majority of public authorities, academic institutions and EU citizens would favour an obligation to release the code developed with public money onto open-source repositories (61%), as well as a common open-source licensing schema across the EU (64%).

Table 4. EU policy measures to support procurement of cloud and AI computing services

Policy Measure	Companies[8]	Public Authorities	EU Citizens	Business associations / trade unions	CSOs[9]
Guidelines with standard criteria to procure cloud services	50%	85%	61%	20%	55%
Standardised tender vocabulary and requirements	38%	54%	36%	20%	30%
Guidelines with standard award criteria	32%	69%	26%	17%	39%
Criterion for solutions with added value and innovation	27%	23%	30%	33%	18%
Improvement of skills and capabilities	32%	69%	41%	40%	21%
Marketplace of cloud and AI computing services	26%	62%	31%	20%	27%
Supporting an open source software ecosystem	62%	31%	92%	73%	60%

[8] In each policy measure, companies include data centre operators, cloud/edge/telecommunications providers, cloud/edge/AI users, AI developers and AI deployers, and financial institutions.
[9] The category Civil Society Organisations (CSOs) include NGOs, consumer organizations, environmental organizations, and academic/research institutions.

In the CfE, some national and local governments as well as several public authorities emphasized empowering public buyers through model clauses and guidance to help public administrations to procure cloud services. However, some warned against mandatory obligations that could conflict with EU procurement principles or overly limit their flexibility.

Some companies framed public procurement as a critical but underused leverage point, though they diverged sharply on solutions. European companies argued that current frameworks fail to empower buyers to choose sovereign, sustainable, or interoperable solutions, calling for uptake targets for trusted EU cloud services and criteria based on sovereignty and environmental performance. Some argued for a diversification of cloud supply, including strengthening EU-based alternatives and governance but without restricting the use of non-EU providers.

In contrast, global providers support the EU's ambitions to bolster innovation and security but warn against overly restrictive sovereignty rules that could hinder competitiveness and limit access to cutting-edge technologies if they exclude providers based on corporate origin. Sovereignty requirement for critical use cases must be carefully defined to avoid fragmentation. They advocate for a pragmatic and targeted approach to defining 'sovereignty' to avoid unintended consequences such as straining the EU's cloud ecosystem or fragmenting the Single Market. To strengthen resilience and avoid vendor lock-in, several companies and business organisations recommend that public authorities adopt multi-cloud strategies for non-critical use cases.

In general, all respondent groups, especially public authorities and both EU and non-EU companies, showed strong support for open source to foster sovereignty, interoperability and competition.

4.4 Lack of common concept and operational criteria for sovereign cloud and AI computing services

In the CfE, respondents consistently identified the absence of a common EU definition and certification framework for sovereign cloud and AI computing services as a fundamental barrier to building trust, driving adoption, and enabling cross-border scalability. The lack of harmonized cybersecurity standards particularly limits providers' ability to scale services across Member States, creating fragmentation that undermines the Single Market potential. This regulatory gap has intensified demands for trusted EU-based cloud providers capable of delivering sensitive data services with robust guarantees of legal and operational sovereignty, interoperability, and protection from extraterritorial interference. These concerns align with public sentiment, as EU citizens expressed significant wariness about foreign control of public data where 85% reported low to very low trust in providers based outside of the EU, and 76% considered public services in the EU should not be allowed to store citizen data with non-EU cloud providers.

In the CfE, there was near-universal agreement that the term 'digital sovereignty' lacks a clear and actionable definition, particularly in the context of cloud and AI computing services. Public authorities acknowledged that the concept of 'sovereign cloud' remains ill-defined, creating uncertainty across the policy landscape. Several EU citizens emphasized that sovereignty should ensure services critical to public continuity cannot be disrupted unilaterally by non-EU actors.

4.1.4 Policy measures

Among public authorities, 77% would support a criterion to ensure sovereignty, autonomy, resilience and availability. In the CfE, public authorities specifically called for a clear, uniform definition of cloud sovereignty that encompasses data ownership, exclusive EU jurisdiction, and comprehensive contractual safeguards. Many advocated for deploying EU-level secure cloud offerings comparable to existing frameworks like SecNumCloud or EUCS High+. Some respondents repeatedly emphasized the urgency of finalising the EUCS certification scheme and integrating it into procurement frameworks, while leveraging public procurement rules to reinforce sovereignty requirements and mitigate national security risks. Several public authorities proposed extending NIS2 scope to include suppliers serving essential public services.

Some public authorities and national governments advocated for functional, risk-based approach to sovereignty as full technological autonomy for all cases is not realistic. Sovereignty should be anchored in clear operational criteria focused on retaining control over data and operations, switching providers, and avoiding undue foreign legal influence rather than mandating EU-only solutions. Regulatory bodies emphasized that sovereignty must not become a pretext for fragmentation, instead advocating for open architectures, multi-cloud approach, and guaranteed access to key inputs for challenger firms.

Among industry associations, there was a split between those calling for functional definitions based on EU legal jurisdiction and vendor independence through federated European solutions, and those warning that overly restrictive criteria could impede cross-border services and harm innovation. Several European companies pushed for enforceable criteria involving EU ownership, legal immunity from third-country laws, and operational autonomy, with some proposing sovereignty frameworks differentiated by use case criticality. In contrast, non-EU providers urged against rigid definitions, recommending non-discriminatory and risk-based criteria grounded in technical safeguards rather than ownership or nationality.

Table 5. Level of support for EU policy measures to protect against unlawful access to sensitive data by third-country legislation with extraterritorial reach and risk associated with supply chain dependencies

Policy Measure	Companies[10]	Public Authorities	EU Citizens	Business associations / trade unions	CSOs[11]
Criterion ensuring sovereignty, autonomy, resilience and availability	45%	77%	63%	23%	52%
Criteria to narrowly identify highly critical use cases for public procurement	30%	62%	48%	20%	52%
Pursue international cooperation with third countries that address such risks	45%	69%	40%	70%	27%
Criteria to differentiate between third countries depending on whether they pose specific threats to the Union	29%	54%	44%	27%	24%

[10] In each policy measure, companies include data centre operators, cloud/edge/telecommunications providers, cloud/edge/AI users, AI developers and AI deployers, and financial institutions.
[11] The category Civil Society Organisations (CSOs) include NGOs, consumer organizations, environmental organizations, and academic/research institutions.

ANNEX 3: WHO IS AFFECTED AND HOW?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

This initiative aims at providing a framework to ensure the functioning of the internal market for cloud and AI computing services in the Union and secure the necessary conditions for the Union's competitiveness and strategic autonomy. The preferred policy options and measures are expected to increase computing capacity deployed in the EU through innovative and sustainable technologies, ensure attractive conditions for the deployment of such computing capacity, decrease the overall reliance on non-European cloud and AI computing services and contribute to the protection of public order by enhancing resilience of supply of cloud and AI computing services in particular for the public sector.

The key stakeholder groups concerned include data centre operators, cloud and AI computing service providers, private sector entities operating in sectors listed under Annex I of NIS2, national and local public authorities, and the European Commission. However, all businesses that rely on digital services across a wide range of sectors, as well as citizens will also be indirectly impacted, albeit in varying degrees. The following table presents an overview of the main impacts and stakeholders affected for the preferred options.

Table 6. Main impacts and stakeholders affected

Affected stakeholder		**Main impacts** **Costs**	**Benefits** (Direct and indirect)
Businesses	Data centre operators	— Direct compliance costs: — Administrative costs (e.g. preparing applications and ensuring compliance with funding rules; paperwork for fast track permitting) — Adjustment costs (e.g. adjustments to meet funding eligibility criteria and access the areas)	— Improved predictability of regulatory direction (e.g. coordination efficiencies and reduced information asymmetries) — Reduced fragmentation of national approaches and administrative simplification, e.g. fewer bilateral interactions, clearer requirements, and coordinated processing — Reduced permitting delays (e.g., faster time to market and higher NPV, labour time saved) — Direct financial support for innovation and deployment — Energy savings — Possibility for improved access to investment opportunities (CAPEX de-risking) — Easier cross-border operations

Affected stakeholder		Main impacts: Costs	Main impacts: Benefits (Direct and indirect)
	Cloud and AI computing service Providers	— Direct compliance costs: — Administrative costs (e.g. providing information for repository; participation to audits; preparation of applications for funding scheme) — Adjustment costs (e.g. alignment with sovereignty criteria; participation to public procurement procedures; eventual alignment with standards)	— Improved predictability of regulatory direction (e.g. coordination efficiencies and reduced information asymmetries) — Reduced fragmentation of national approaches — Reputational gains from alignment with EU standards — Easier cross-border operations — Faster procurement — Direct financial support for innovation — Improved access to investment opportunities — Reduced marketing costs — Increased revenues — Easier uptake of innovative solutions for cloud and AI computing services — Productivity gain and business modernisation — Improved business continuity
	Private sector entities operating in sectors listed under Annex I of NIS2	– Direct compliance costs: — Administrative costs (i.e. expanded cybersecurity risk assessment to address non-technical risks)	
Public authorities	National and local public authorities	— Direct compliance costs: — Administrative costs (e.g. data collection of fast-track areas; sovereignty risk assessments; drafting of national strategies; updates of procedures/ templates related to public procurement; reporting activities to maintain the open source programme office and on the implementation of national strategies) — Adjustment costs (e.g. redesign of permitting processes and reprioritising planning resources for fast-track areas; alignment of national measures with EU-level rules; integrating risk assessment outcomes within procurement; transition costs linked to new cloud and AI computing services providers; participation in the public sector cloud federation; alignment of procurement criteria; set up and management of the infrastructure for the open-source repository)	— Enhanced dialogue with industry — Better monitoring of sector developments — Alleviated constraints and delays resulting in reduced pressure from industry over bottlenecks — Reduced time dedicated to individual data centre projects — Saved effort from common mechanism and sharing of idle capacity — Faster and more reliable procurement processes — Reduced screening efforts and efforts needed to verify eligibility — Streamlined verification of compliance — More sovereign cloud and AI computing services — Reduction of proprietary license expenditures and lower licensing costs — Reduced duplication of work and efforts — Reduction of total cost of ownership for IT systems — Shorter procurement time for innovative solutions; reduced time needed to find providers

Affected stakeholder		Main impacts: Costs	Main impacts: Benefits (Direct and indirect)
	European Commission	— Administrative costs (e.g. design and monitor EU-level funding instruments; setting up and overseeing the repository of audited sovereign services; financial and coordination support) — Adjustment costs (e.g., setting targets; monitoring progress; new supervisory capacity to enforce EU-level targets; design of training programme; setting up the certification framework; developing and deploying the federation platform; setting up the voucher scheme for SMEs; setting up the cloud and AI toolbox) — Enforcement costs (e.g. running EU-level infrastructure, defining targets and ensuring compliance)	— Harmonisation of practices and approaches across the EU — Increased ability to steer the market towards EU priorities and accelerated innovation — Reduced duplication of efforts at national level — Faster and more reliable procurement processes; — Reduced screening efforts and efforts needed to verify eligibility; — Streamlined verification of compliance; — Reduction of proprietary license expenditures and lower licensing costs; — Reduced duplication of work and efforts; — Reduction of total cost of ownership for IT systems; — Shorter procurement time for innovative solutions; reduced time needed to find providers
Consumers and citizens	Consumers and citizens	— Potential budgetary trade-offs from public funding — Possible cost pass-through from compliance obligations to end users — Higher prices[12]	— Improved transparency and stakeholder engagement — Faster and more sustainable roll-out of digital infrastructure — Improved digital service quality and lower costs — Improved transparency on security properties — Enhanced protection of fundamental rights, especially privacy and data protection — Enhanced transparency and trust — Higher employability — Greater trust in public digital services

[12] Concerning data centre expansion, potential increased costs via grid tariffs are an important element. ACER's 2024 Electricity Infrastructure Monitoring Report shows that future grid costs are highly sensitive to rising electricity consumption and increased grid-investment expenses, with a 10% increase in either factor possibly resulting in a 1 to 4.5 EUR/MWh rise in grid costs by 2050. As data centres are among the fastest-growing and electricity-intensive sectors, they influence both drivers of higher grid costs with consequent possible increases in electricity prices. The Finnish National Roadmap for Data Centres similarly highlights that the sector's expansion could strain the power grid and contribute to higher electricity prices unless data centre development and grid planning are coordinated proactively. See also: Overcoming energy constraints is key to delivering on Europe's data centre goals – Analysis - IEA; ACER Monitoring Report on cross-zonal electricity trade and congestion management in the EU (2025) and National Roadmap for Data Centres : Rapporteur's Report.
Moreover, in regions where water resources are limited, inefficiently managed industrial demand can exacerbate competition with households, increase the likelihood of water restrictions, and call for expensive network upgrades – costs that may ultimately affect consumer water bills depending on the tariff structure and regulatory cost distribution. Thus, proactive governance of data centre water usage is also key to protect citizens' access to water and prevent unintended increases in residential water costs.

Affected stakeholder	Main impacts Costs	Benefits (Direct and indirect)
		— Continuity and resilience of critical services, like health, defence, and finance

This initiative is expected to generate costs for data centre operators and cloud and AI computing service providers, but also significant savings and direct economic benefits. While administrative and adjustment costs arise from, *inter alia*, participation in funding programmes and fast-track permitting procedures, or from the audit procedures and risk assessments, these are offset by the efficiencies and benefits that emerge from administrative simplification, reduced fragmentation of national approaches, and greater incentives for investments, improving the attractiveness of the Single Market.

National public authorities are expected to incur administrative and adjustment costs for assessing applications for support measures and permitting, planning resources for fast-track areas, monitoring compliance, and participating in the cloud federation. However, these costs are balanced by significant savings resulting from reduced inefficiencies and duplications caused by the lack of harmonisation. National public authorities will also directly benefit from open source solutions as well as indirectly from additional cloud and AI capacity at lower costs. Ultimately, this initiative aims to support the digital transformation and resilience of public authorities. Moreover, while some Member States might need a reinforcement of capabilities, the EU would bear the cost of oversight, with the aim to create efficiency gains in the cooperation across Member States. The administrative and adjustment costs borne by the European Commission**,** related to the implementation of the measures and their supervision are expected to be outweighed by significant long-term benefits. Society at large is expected to benefit from the wider availability of digital services, underpinned by robust digital infrastructures. As the same time, the deployment of sustainable infrastructures will accelerate the green transition, ensuring that digitalisation goes hand in hand with environmental responsibility.

The assessment of the impacts draws on multiple data sources, including the targeted stakeholder consultation (interviews and surveys), the public consultation, and desk research in the context of the impact assessment support study. To the extent possible, the impacts are quantified based on available assessments or modelling by Technopolis et al. (2025)[13]. Where dedicated modelling was not possible due to the lack of tools or data, a qualitative assessment was performed, based on existing studies and input from stakeholders. Annex 4 provides further details on the methodological approach, detailed tables and estimates.

2. SUMMARY OF COSTS AND BENEFITS

I. Overview of Expected Benefits (total for all provisions) – Preferred Option		
Description	***Indicative range*** *(NPV 10-years)*	***Comments***
	Direct benefits	
Economic benefits from administrative simplification and fast-track areas for providers (PM4, PM5)	EUR 8 – 27 bn	These are the large, expected benefits accruing to data centre operators which are foreseen to benefit from reduced times to build new facilities. It has been calculated as the net present value of discounted economic benefits over 10 years. The economic benefits that are expected from these measures extend beyond the measurable impact (see below on indirect benefits).

[13] Technopolis et al. (2025), “Study: Cloud and AI”

Cost savings from administrative simplification and fast-track areas for public authorities (PM4, PM5)	EUR 166 – 277 m	These include administrative cost savings accruing to public administrations as they reduce parallel processing of projects and back-and-forth interactions with operators.
Cost savings from the increased use of open source in public administrations (PM20)	EUR 2 – 12 bn	By reusing and adapting existing software rather than commissioning bespoke solutions, administrations can reduce duplication of effort and lower the total cost of ownership of ICT projects.
Costs savings for authorities from using standard non-specific award criteria when drafting tender specifications (PM19)	EUR 4 – 13 m	Cost savings for public authorities stem from use of standard criteria when procuring cloud and AI computing services that can be reused across all public tenders.
Costs savings for authorities from using audited services in tenders (PM21)	~ EUR 2.5 m	Cost savings for public authorities stem from the use of the repository of sovereign cloud and AI computing services and audit reports, which are expected to save administrations time in their verification of the documentation for the evaluation of the offers.
Cost savings for cloud and AI service providers from being able to use sovereignty audits across all MS, i.e. once and for all (PM21)	EUR 2 – 5 bn	These direct savings for providers stem from their ability to get the audited in one Member State and participate in procurement of services for critical use cases across all EU27.
Cost savings from cloud federation and joint procurement for public administrations (PM22)	EUR 19 – 49 bn	Recurrent savings stem from the cloud federation, i.e. from reducing idle capacity, getting cheaper computing resources and reducing the coordination effort for sharing computing capacity. The participation in the joint procurement framework and the aggregation of demand in common EU-level procurement processes is also expected to significantly reduce the required FTEs for procuring cloud and AI computing services and service prices from higher scale and purchase power.
Direct cost savings in AI-based transformation project design for SMEs (PM23)	EUR 160 – 500 m	The targeted scheme to provide financial support to SMEs for adopting cloud and AI computing services foresees a yearly budget of EUR 40 050 000 over the 10-year period, mostly dedicated to supporting the design and planning phase of cloud and AI-based transformation projects for SMEs. The grants are fixed amounts that SMEs can spend in consultancy services to design digital transformation projects based on cloud and AI technologies.
Indirect benefits		
Indirect benefits coming from data centre deployment targets	This was assessed qualitatively or based on existing literature.	Decrease of the capacity gap and contribution to the overall GDP and workforce driven by the data centre sector and related fields. For operators, clearer EU-wide targets and consistent monitoring could help reduce investment uncertainty, reducing effort in oversupplied or poorly sited locations. National authorities would also benefit from improved infrastructure foresight, with better planning for grid reinforcements and targeting of support schemes.
Indirect benefits from additional data centre capacity on GDP growth and employment levels	This was addressed under Section 6.1.5 and 6.2.	Economists have attributed the growth in GDP growth from investment in data centres and information processing technology[14]. In additional to these gains, there are likely to be indirect benefits for society at large, e.g. in terms of improved digital infrastructure, skills development and increased attractiveness of the EU for complementary industries. These spillover effects, while possibly significant, are not directly quantified due to the lack of reliable data.

[14] Harvard economist Jason Furman reported in September 2025 that investment in information processing equipment & software was 4% of GDP in the US in 2024, but it was responsible for 92% of GDP growth in the first half 2025; US GDP excluding these categories grew at a 0.1% annual rate in the first half of 2025. More information available here: Without data centers, GDP growth was 0.1% in the first half of 2025, Harvard economist says | Fortune.

Indirect benefits coming from funding for R&D and strategic projects	This was assessed qualitatively or based on existing literature.	It is important to underline that the expansion of data centre capacity entails considerable environmental impacts, including increased energy consumption, water use, land uptake and associated carbon emissions. These impacts may generate new social and environmental costs, with possible consequences for overall welfare, local ecosystem and community acceptance. For these reasons, measures that promote sustainable solutions are fundamental to ensure that new facilities are designed and operated with sustainability principles at their heart. This fundamental to maximise net social benefits and safeguard the public good over the long term.
Indirect benefits from the increased use of open source solutions in public administrations	This was assessed qualitatively or based on existing literature.	When public administrations increase their procurement and use of open source software, they create additional demand for open and interoperable solutions across the wider economy.
Indirect benefits from the sovereignty risk assessment scheme	This was assessed qualitatively or based on existing literature.	The 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. It 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. At the same time, it contributes to reducing exposure to non-EU dependencies and single provider concentration risks, strengthening the resilience and autonomy of cloud and AI services.
Indirect benefits from joint EU-level procurement	This was assessed qualitatively or based on existing literature.	The increase in public procurement of cloud and AI sales volume that is addressable by European providers may help increase their scale and competitiveness and their share in the European and global cloud and AI markets.

(1) Estimates are gross values relative to the baseline for the preferred option as a whole (i.e. the impact of individual actions/obligations of the preferred option are aggregated together); (2) In the comments column the key stakeholder group as main recipient of the benefit is presented;(3) Spillover effects and broader social benefits of enhanced digital infrastructure for citizens and consumers were hard to quantify given their long-term and diffuse nature and were thus assessed only qualitatively.

II. Overview of expected costs, indicative ranges as discounted NPV over 10 years – Preferred option							
		Citizens/Consumers		**Businesses** (including SMEs)		**Administrations** (national public and European Commission)	
		One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
Legislative and financial intervention enforced nationally: Administrative simplification and fast-track areas for the roll-out of data centres; support measures and deployment targets also based on national data centre strategies (PO1-B)	Direct adjustment costs			EUR 6 – 26 m		EUR 28 – 43 m	EUR 2 – 14 m
	Direct administrative costs			EUR 1 – 4 m	EUR 0.2 – 0.6 m	EUR 1 – 6 m	EUR 46 – 86 m
	Direct enforcement costs						EUR 30 – 89 m
EU R&D funding and deployment funding for strategic projects (PM8, PM9)	Direct adjustment costs					EUR 1 – 2 m	EUR 0.6 – 1.2 m
	Direct administrative costs			EUR 1 – 3 m			

II. Overview of expected costs, indicative ranges as discounted NPV over 10 years – Preferred option							
		Citizens/Consumers		**Businesses** (including SMEs)		**Administrations** (national public and European Commission)	
		One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
EU-coordinated procurement and support framework for sovereign cloud and AI computing services: OSS use in the public sector; mandatory use of audited cloud and AI computing services in highly critical public sector use cases and award criteria; private entities cybersecurity risk-assessment integration to consider risks from using non audited providers; national strategy definition and monitoring; joint EU-level procurement; public sector cloud federation; SME support scheme; Cloud and AI toolbox (PO2-C)	Direct adjustment costs			EUR 173 m – 352 m		EUR 140 m – 420 m (*)	EUR 1.3 – 2.7 bn
	Direct administrative costs			EUR 27 m – 83 m	EUR 560 m – 2.9 bn	EUR 10 m – 27 m	EUR 142 m – 293 m
	Direct enforcement costs						
	Direct regulatory fees and charges			~ EUR 3 m	~ EUR 3.4 m		

(*) The mandatory use of sovereign cloud and AI computing services would trigger an acceleration of porting of some applications to sovereign cloud services of assurance levels 2 to 4, requiring an anticipation of expenses of EUR 3 to 15 bn, as reported in section 12.4 of Annex 4. Since they represent planned expenditure that would be incurred in the future as part of the regular cloud contract renewal cycles and independent of the preferred option, they have been scoped outside of the summary cost table so as not to conflate structural renewal costs with the incremental financial impact of the measure itself.

(1) Estimates (gross values) to be provided with respect to the baseline; (2) costs are provided for each identifiable action/obligation of the preferred option otherwise for all retained options when no preferred option is specified; (3) If relevant and available, information on costs is presented according to the standard typology of costs (adjustment costs, administrative costs, regulatory charges, enforcement costs, indirect costs;); (4) although relevant environmental and social costs have been considered in this assessment, they were not quantified here due to the lack of sufficient and reliable data.

III. Application of the 'one in, one out' approach – Preferred option			
	One-off (annualised total net present value over the relevant period)	**Recurrent** (annualised total net present value over the relevant period)	**Total**
Businesses			
New administrative burdens (INs)	(EUR 30 m – 90 m)	(EUR 559 m – 2.8 bn)	(EUR 589 m – 2.8 bn)
Removed administrative burdens (OUTs)		EUR 404.3 – 2 bn	EUR 404.3 – 2 bn

III. Application of the 'one in, one out' approach – Preferred option			
	One-off (annualised total net present value over the relevant period)	**Recurrent** (annualised total net present value over the relevant period)	**Total**
Net administrative burdens*	(EUR 30 m – 90 m)	(EUR 154.7 m – 0.8 bn)	(EUR 184.7 m – 809 m
Adjustment costs**	(EUR 179 m – 378 m)		
National public administrations			
New administrative burdens (INs)	(EUR 12 m – 34 m)	(EUR 154 m – 414 m)	(EUR 166m – 448 m)
Removed administrative burdens (OUTs)		EUR 90 m – 154 m	EUR 90 m – 154 m
Net administrative burdens*	(EUR 12 m – 34 m)	EUR 64 –2-60 m	EUR 68 m – 194m
Adjustment costs**	EUR 209 m –507 m	EUR 1 bn – 3 bn	
Total administrative burdens***	***EUR 42 m – 124 m***	***EUR 218.7 m – EUR 860 m***	**EUR 252.7 m –1.00 bn**

(*) Net administrative burdens = INs – OUTs;
(**) Adjustment costs falling under the scope of the OIOO approach are the same as reported in Table 2 above.
(***) Total administrative burdens = Net administrative burdens for businesses + net administrative burdens for public administrations

3. RELEVANT SUSTAINABLE DEVELOPMENT GOALS

IV. Overview of relevant Sustainable Development Goals – Preferred Option		
Relevant SDG	**Expected progress towards the Goal**	**Comments**
e.g. SDG no. 4 – quality education	Increase in training opportunities for enhancing digital skills, contributing to quality education and lifelong learning.	
e.g. SDG no. 7 - affordable and clean energy, 12 - responsible consumption and production, 13 - climate	Increased energy efficiency of data centres will save energy and CO_2e emissions per GW of additional capacity added with respect to the baseline over the next 10 years, contributing positively to SDG no. 7 (affordable and clean energy) and SDG no. 13 (climate action) including through the promotion of renewable energy sources to power data centres. Greener data centres would contribute to reduce their carbon footprint and support the clean energy transition. Promotion of energy-efficient hardware and optimisation of cooling systems, also thanks to the use of AI-integrated solutions, is also expected to reduce waste and resource consumption. The proposal embeds the concept of "sustainable-by-design" data centres, including high environmental and energy-efficiency obligations, e.g., through alignment with the upcoming Union scheme for rating the sustainability of data centres.	Affordable energy for all must be sustained through the renewal and upgrade of the energy grids (which falls outside of the scope of the current initiative), but which is a relevant prerequisite to move closer to this SDG target.

IV. Overview of relevant Sustainable Development Goals – Preferred Option		
Relevant SDG	**Expected progress towards the Goal**	**Comments**
SDG no. 8 – Decent work and economic growth	Expected increase in employment in relation to data centre rollout and GDP growth. Expected increase of SMEs and startups' use of cloud to support inclusive economic growth.	
SDG no. 9 – Industry, innovation and infrastructure	Increase in the number of data centres and next generation infrastructure to meet the needs of business and citizens in the EU, strengthen innovation and build resilient digital infrastructure.	Cloud computing and AI also enable digital transformation across industries, boosting productivity and new services. The initiative aims to increase the EU's share in the global cloud market from 15% to 30%.

ANNEX 4: ANALYTICAL METHODS

1. METHODOLOGY

This impact analysis has followed a stepwise approach.

First, a **modelling analysis** of each proposed policy measure has been carried out, using a structured set of parameters, assumptions and data inputs[15]. The data included has been gathered from the following sources:

- Eurostat, notably for the labour costs.
- The supporting study "Study: cloud and AI" led by Technopolis Group[16], including over 60 targeted interviews, surveys with over 250 replies and two workshops with over 100 participants each.
- Tenders Europe Daily (TED), for the calculation of the procurement contract values by public administrations in the field of cloud and AI computing services.
- Desk research, with sources cited in the corresponding measures.
- Best practices documented in the industry or similar approaches followed in other world regions or in EU countries.

Section 2 of this Annex explains the general assumptions used for the modelling of the different policy measures. These assumptions apply across several policy measures and are therefore reused throughout the analysis.

Section 3 includes a detailed explanation of the modelling approach for each policy measure. For each measure, the analysis covers:

- The scope of the policy measure and how it would be implemented in practice.
- The different types of costs, including the one-off and recurrent administrative and adjustment costs per stakeholder
- The assumptions, values and sources used to estimate these costs.
- The expected cost savings and benefits, including the assumptions and the reasoning behind them.
- Where relevant, indirect savings, that cannot be fully monetised, but that nevertheless play an important role for assessing the overall effect of the policy measure.

A sensitivity analysis was carried out to identify the parameters with the greatest variability and the strongest potential impact on the cost-benefit results. This analysis helps understand the robustness of results under the different assumptions. A final summary table presents the overall results for each policy measures, under three scenarios (central-min-max), as well as costs and benefits for the key stakeholder groups impacted.

The modelling has resulted in a cost-benefit analysis for each policy measure, which was aggregated and presented in sections 6 and 7 of the core text of the impact assessment and in the Annex 3. In most cases, the analysis followed the Standard Cost model, whereas in some instances the NPV or other quantification approaches have been used to estimate expected benefits.

---

[15] This consisted of a cost-benefit model built around defined assumptions and evidence sources, not on a macroeconomic model.

[16] Technopolis et al. (2025). "Study: Cloud and AI"

Section 4 discusses the strengths and limitations of the approach and of the data used for the analysis. To investigate the robustness and stability of the results, a min-max **sensitivity analysis** was performed (See section 5 of this Annex for more details and assumptions checked in interviews and CATI surveys).

Section 6 presents the **multi-criteria decision analysis (MCDA)**, which was carried out using three different models, to further assess the strengths and weaknesses of each option.

Wider economic impacts, indirect effects or non-market social and environmental externalities can be material but are excluded from the monetisation within the Cost-Benefit Analysis due to limitations in available data and the lack of robust methodologies for monetising these effects.

Section 7 of this Annex includes the assumptions behind the environmental impact analysis performed, while section 8 includes additional literature used to discuss the wider economic effects associated with the policy options.

Section 9 shows the analysis performed by Technopolis Group as part of the study "Study: cloud and AI" on the different procedures, permits and data centre deployment timelines across several Member States, aiming to demonstrate the fragmented approach currently existing in the EU.

2. General assumptions for the modelling of the policy measures

2.1. Valuation framework and time horizon

Price base. All figures are expressed in real 2025 euros; no general price inflation is applied. All unit costs are expressed in real 2025 euros and are based on Eurostat hourly labour cost. In 2024, the EU-27 average hourly labour cost for the whole economy was EUR 33.5; services averaged EUR 33.3; information and communication at EUR 46.3; and the mainly non-business economy (excl. public administration) averaged EUR 34.2. These figures are taken from Eurostat's latest annual release and Statistics Explained pages[17].

Discounting. Present values are computed at a 3% real discount rate. The discounting base date is the beginning of 2027; cash-flow timing follows an end-of-year convention. The cumulation period is 2027-2036 inclusive. The discount factor for a flow in year *t* is:

$$\mathrm{DF}_t = \frac{1}{(1+0.03)^{t-2027}}$$

Horizon. Impacts are accumulated over 2027–2036 inclusive (10 years).

2.2. Unit cost parameters/ standard cost model

Working day length. 8 hours/day.

Working days in the year. 220 working days/year

Day-rate proxies (EU averages with sector uplifts):

Eurostat's EU-27 hourly labour cost converted to day-rates:

[17] EU hourly labour costs ranged from €11 to €55 in 2024 - News articles - Eurostat

Table 7. Labour costs and rates used (Source: Eurostat and Statistics Explained Hourly labour costs page (Table for breakdown by activity)

Baseline aggregate	**Hourly labour cost** (2024, EU-27)	**Day-rate** (8h)
Services	EUR 33.3 / h	EUR 266.40 / day
Mainly non-business (excl. public admin)	EUR 34.2 / h	EUR 273.60 / day
Information and communication	EUR 46.3/h	EUR 370.40 / day

Eurostat's 2024 reports, for the EU-27, an average hourly labour cost in Information and communication (NACE J) at EUR 46.3/hour[18]. This level reflects the high ICT skill mix and sits above the overall services economy. Anchoring directly to NACE J provides a relevant comparator for data-intensive activities. To capture systematic differences in skill composition and overhead, modest multipliers are applied to the J baseline, justified by reports on ICT labour market tightness and hard-to-fill vacancies[19]. Each uplift is a **modelling parameter**, justified by EU evidence on sector pay premia and administrative overheads:

- **Cloud service providers (CSPs):** ICT activities (NACE J62 – Computer programming, consultancy, and related activities; J63 – Information service activities) carry higher earnings and labour costs than services overall due to specialist roles (software engineers, site reliability engineers, cybersecurity). Eurostat SES shows ICT employees are concentrated in higher-skill/tertiary categories; Eurostat reports tight markets for ICT specialists and persistent hard-to-fill vacancies, supporting a positive premium vs. average services. A 30% uplift is set on this baseline, which yields to EUR 481.52/day (46.3×8×1.3)

- **AI computing service providers:** AI computing service providers offer computing infrastructure for the running (inference) of AI systems. Due to the complexity and novelty of running these clusters of AI GPUs, more specialised roles are needed compared to those running cloud infrastructures. Data show employees in these groups cluster in the highest wage deciles within ICT and Eurostat reports structural labour shortages in ICT that are particularly acute for advanced digital skills. This systematic premium reflects both scarcity of talent and high value-add of AI services compared with broader ICT[20]. A 45% uplift is set on the baseline, which yields to EUR 537.08/day (46.3×8×1.45)

- **Data centre operators:** DC operations mix technical operators, electricians, facility engineers and IT technicians. The mix is more operations-heavy and less developer-heavy than CSP software teams, so the premium over services is lower than for CSPs but still positive relative to the broad aggregate due to 24/7 operations and specialised compliance (e.g., uptime, safety). A 8% uplift positions DC operations below CSPs but above average ICT services, consistent with observed role mixes in NACE J63.11. This +8% leads to EUR 400.03/day (46.3×8×1.08).

- **National public authorities:** Eurostat does not publish NACE O separately in this dataset, but reports EUR 34.2/h for the "non-business economy excl. O" aggregate, with

[18] [lc_lci_lev] Labour cost levels by NACE Rev. 2 activity
[19] ICT specialists in employment - Statistics Explained - Eurostat
[20] AI Jobs Barometer | PwC

a figure for the mainly non-business economy (excl. public administration) as EUR 34.2/h. We apply a small +5% uplift to proxy: (i) policy/project staff engaged in inter-institutional coordination (above average non-business roles), and (ii) inclusion of specialist grades not perfectly captured by the “excl. public administration” aggregate. This remains conservative relative to some MS where public-sector employer costs are higher than the EU average. This +5% on non-business (excl. public admin) leads to EUR 287.28/day (34.2×8×1.05).

- **European Commission:** Coordination at EU level entails multilingual drafting, legal vetting, translation, dissemination, and inter-DG and MS engagement. Relative to Member-State averages for non-business activities, Commission project teams typically face higher overhead (procurement, quality assurance, inter-service consultation). The +15% factor is a policy-evaluation convention to reflect those overheads while staying close to EU-wide non-business costs. Using the baselines and multipliers above +15% on non-business (excl. public admin) leads to EUR 314.64/day (34.2×8×1.15).

- **Private sector essential entities operating in sectors listed in Annex I of NIS2:** Annex I NIS2 lists the following sectors as highly critical sectors: Banking and Financial market infrastructures (NACE Rev2 - K), Health (NACE Rev2 - Q), Drinking Water and Waste water (NACE Rev2 - E). Energy (NACE Rev2 - D), Transport (NACE Rev2 – H), Digital infrastructure and ICT Service Management (NACE REv2 - J), Public Administration and defence (NACE Rev2 – O) and Space (NACE Rev2 – C). The values that Eurostat yields for this query for 2024, the most current data is 46.8 €/hour[21]

Using the baselines and multipliers above

- CSPs: 46.3 EUR /h×8×1.30 = EUR 481.52 / day.
- Data-centre operators: 46.3 EUR /h×8×1.08 = EUR 400.03 / day.
- AI service providers: 46.3 EUR /h×8×1.45 = EUR 537.08 / day
- National authorities: 34.2 EUR /h×8×1.05 = EUR 287.28 / day.
- European Commission: 34.2 EUR /h×8×1.15 = EUR 314.64 / day.

External contractor rates: are set at 50% over external AI developer, EUR 537.08/day x 1.5= EUR 805,62/day.

Travel. EUR 700 per in-person trip per participant (transport and incidentals for one day and one night).

Webinars. 2 hours per participant, converted to 0.25 day for labour costing.

In-person meeting/event time. Each in-person engagement entails 2.5 participant-days (1.0 meeting days + 1.5-day for preparation and follow-up).

2.3. Estimates related to data centres

2.3.1 Data centre supply growth

There is no single, EU-wide dataset produced by regulators or energy system planning exercises that consistently locates historical data centre capacity at site level in terms of commissioned

[21] Query used available at https://ec.europa.eu/eurostat/databrowser/view/lc_lci_lev__custom_20086615/default/table

IT load. The estimation of new data centres deployed under the different policy options builds on the scenarios of data centre growth (measured in MW) identified in Technopolis et al. (2025), "Study: Cloud and AI". The analysis relied primarily on the Data Centre Map dataset, which is built entirely on historical data centre sites that have already been developed and commissioned, i.e. the 2025 dataset reflects the cumulative outcome of past capacity development rather than a forward-looking projection. The dataset includes the year of launch of the sites for only around one-third of the recorded sites, with uneven coverage across countries and operators. As a result, it was impossible to construct a consistent historical baseline of commissioned capacity across the EU without strong assumption or a systematic bias.

Nevertheless, to present forward-looking projections based on past[22] and future trends, the study estimated possible forecasts for data centre capacity across the EU27 based on the characteristics of three strategic scenarios (low growth, central growth and high growth). These projections illustrate the potential evolution of installed capacity over the next decade, reflecting variations in natural resources, demand drivers, policy intervention, technological innovation, and market responsiveness.

Table 8. Overview of low growth, central and high growth scenarios (Source: Technopolis et al. (2025))

Scenario	CAGR (2025-2036)	Key assumptions and trends
Low growth	9%	• Across 2025–2036, EMEA data centre capacity grows at an average ~9% CAGR, below the ~13.8% historic pace seen in 2018–2024. Growth remains concentrated in primary markets e.g. Germany, France, Ireland, and the Netherland while many secondary and emerging markets struggle to secure large, anchor-tenant investments or hyperscale commitments. The build-out is most intense in 2025–2030 (approximately 14% CAGR), driven by committed pipelines, cloud region rollouts, and AI-ready retrofits. From 2030–2036, momentum slows to roughly 4.2% CAGR as power, permitting, and capital discipline increasingly constrain new capacity additions. • Power availability is the binding constraint, with insufficient electrical capacity to support large-scale AI compute in countries such as Netherlands, Ireland, Germany with limited investment in grid modernisation, increasingly observed between 2030-36. These constraints limit the development of new high-density sites and delay infrastructure upgrades. • In the absence of major policy shifts, a fragmented regulatory landscape persists across Europe. Disjointed national strategies, coupled with tightened environmental restrictions on energy usage and prolonged permitting processes, create significant barriers to new data centre development. These

[22] To contextualise historical growth dynamics we performed desk research and looked at past industry-level analyses, which document that the FLAP-D markets experienced a 17% CAGR in MW supply between 2018 and 2023, while secondary European markets saw a 23% CAGR in the same period. Other industry market reports tracked data centre power capacity and trajectories, showing an increase from 9 GW in the early 2020s to above 11 GW in 2024. These trends confirm the growth dynamics of the European market identified in the study, but they often differ substantially in geographic scope (e.g. considering the EMEA or UK market). No existing study combines the uses a methodology in a comparable manner to that of our study, making any comparisons misleading. See: Roland Berger and spotlight-eu-data-centre---november-2022-.pdf; spotlight-eu-data-centre---may-2024---final.pdf

Scenario	CAGR (2025-2036)	Key assumptions and trends
		hurdles constrain growth, keeping capacity expansion below historically observed levels.
Central growth (used as baseline)	12%	• Capacity growth aligns with the CATI survey average (~13% CAGR) and broader industry momentum through 2025–2030, then eases over 2030–2036. Expansion remains concentrated in FLAP-D hubs, with steady investment in secondary markets (Nordics, Spain, Italy) and slower uptake in developing markets (around 6.49% CAGR). In the baseline, aggregate growth is ~17.7% over 2025–2030 (consistent with the survey's ~13% CAGR lens) as committed pipelines, AI-readiness upgrades, and new cloud regions come through. From 2031–2036, growth moderates to ~7.1%, reflecting tighter site selection driven by power and land availability, longer permitting lead times, and higher financing costs. • Electrical grid limitations remain an issue in certain primary markets such as Ireland and the Netherlands. However, regulators and operators in several markets have begun investing in grid modernisation and demand management. • Policy evolution remains gradual and inconsistent, creating a fragmented regulatory landscape across Europe. Efforts to modernise infrastructure and streamline permitting are underway, but progress is uneven, often slowed by regulatory complexity and localised decision-making. Governments aim to balance digital infrastructure expansion with environmental priorities by introducing power efficiency targets, and sustainability requirements.
High growth	15%	• The growth rate accelerates to 15% from 2025-2036 with front loaded 21.7% CAGR in 2025-2030 before moderating to 10.4% from 2030-36. This is improving on the baseline scenario by following the trajectory of advanced, leading-edge markets such as Northern Virginia in the US, where data centre capacity grew at a 25% CAGR between 2014 and 2021, with capacity doubling from 2018 to 2021[23]. This scenario sees aggressive geographic expansion beyond primary and secondary markets, with new regional hubs emerging in Southern Europe, the Baltics, and Central & Eastern Europe. Growth in developing regions significantly exceeds historical trends with a CAGR of 13% and outpaces current market projections. • Major public and private investment in grid modernisation leads to substantial increases in available electrical capacity, effectively removing power availability as a constraint on data centre expansion. This enables large scale AI deployments, including high density GPU workloads to

[23] NVTC (2022). The impact of data centres on the state and local economics of Virginia 2022. Available at: https://www.spotsylvania.va.us/DocumentCenter/View/29411/2022-Virginia-Data-Center-Report--32022?

proceed rapidly not only in primary markets but in secondary and developing markets.

- Proactive, coordinated policy action is witnessed across Europe. National and EU-level governments prioritise digital infrastructure development, implementing supportive strategies such as AI innovation hubs, tax incentives, and expedited permitting processes. Environmental goals are addressed in parallel, but through mechanisms that encourage rather than restrict growth, such as mandates for renewable energy procurement and circular economy initiatives.

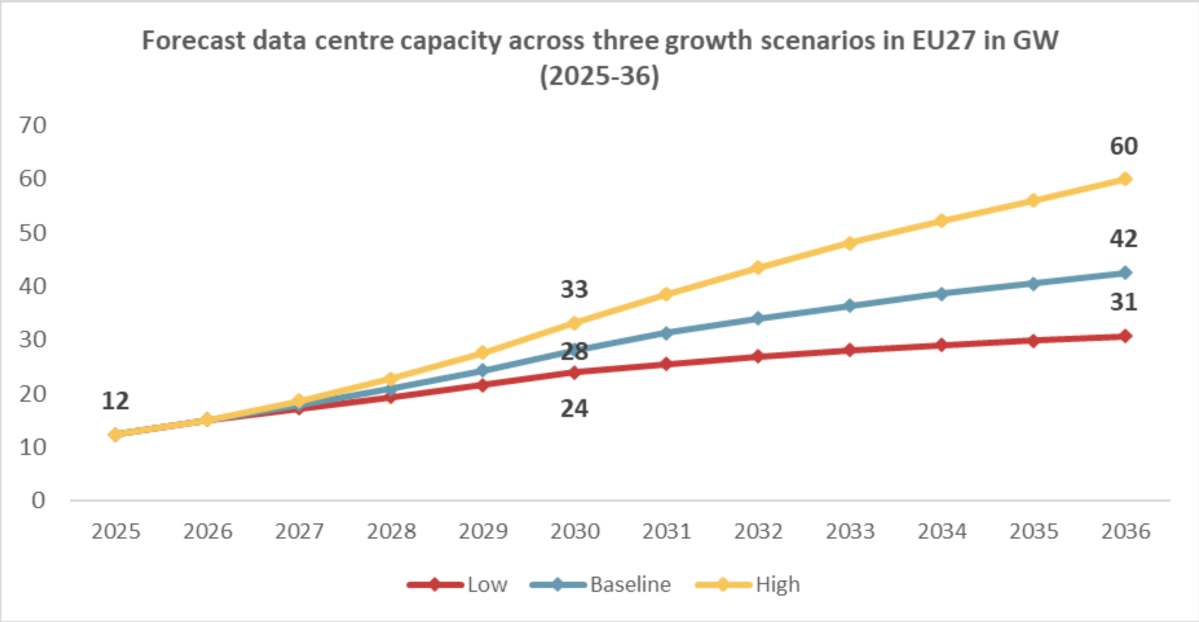
As of 2025, all three scenarios converge at an estimated 12.4 GW of installed data centre capacity. This uniform starting point persists into 2026, with all paths reaching 15.1 GW, based on relatively firm visibility of near-term buildout plans and permitted sites. However, the trajectories begin to diverge thereafter as each scenario follows the key assumptions outlined above from 2027 onwards. This projection broadly aligns with the literature, even though some sources present slightly less ambitious estimates, such as a forecasted capacity of 13.1 GW by 2027[24].

By 2030, under the central scenario, capacity reaches 28 GW. In the high growth scenario, driven by heightened demand and accelerated infrastructure deployment, capacity increases more sharply to 33 GW. Meanwhile, the low growth scenario sees more modest expansion, with capacity reaching just 24 GW by the end of the decade. The CAGR from 2025-36 for the low growth scenario is 9%, for the central growth scenario is 12% and for the fast growth scenario is 15%.

Extending the forecast horizon to 2036 introduces a higher degree of uncertainty, largely due to evolving market dynamics, potential technological breakthroughs, and a lack of visibility into planned or in-progress developments beyond the 2026–2030 window. That said, the divergence between the scenarios becomes more pronounced. In the low growth scenario, installed capacity reaches 31 GW, while the central trajectory leads to 42 GW. The high growth scenario sees capacity expand dramatically to over 60 GW, representing a 55% increase over the central forecast, as shown in the Figure below.

[24] Savills (2024). European data centre power capacity projected to rise to approximately 13,100 MW by 2027. Available at: https://www.savills.co.uk/insight-and-opinion/savills-news/362723-0/european-data-centre-power-capacity-projected-to-rise-to-approximately-13-100-mw-by-2027

Figure 1. Data centre capacity across the EU27 in GW from 2025-36 across three growth scenarios



Source: Technopolis et al. (2025) by means of a CATI survey (n=100 companies, 280 Data Centres), DataCentreMap

These findings complement existing literature, which forecasts a rapid growth in European data centre capacities in the coming years driven by the breakthrough of AI[25]. While a diversification of data centre markets is similarly expected, the literature places more emphasis on constraints affecting the growth of emerging markets, including limited power grid capacity and less developed economic or business ecosystems[26].Technologies typically follow an S-curve growth rate and so is the expectation about data centre growth, implying that at some point in the future, the CAGR will start declining. The study has modelled a partial inflection of growth rates after 2030 but finds that other inflexion points are not expected in the time horizon contemplated here.

To estimate near-term growth, the Data Centre Map dataset was leveraged, since it includes site-level information of facilities "Under Construction" and "Planned." All data centres identified as "Under Construction" were assumed to be operational by 2026, reflecting standard build timelines and aligning with industry expectations. Facilities classified as "Planned" were incorporated into our longer-term forecasts, with their capacity distributed evenly across the 2026–2030 period. Information from government sources, company announcements, and market reports has been consulted to cross-check against these estimates. These sites were then assigned to NUTS-1 regions through geospatial mapping and manual checks where coordinates are missing. Projections beyond 2027 are also adjusted for regional and market maturity categories (primary, secondary, developing) across the three scenarios.

To assess the realism of projected capacity, a natural resource constraint at the NUTS 1 level was incorporated. This was based on the national electricity generation capacity from 2020–2024 available from the European Commission's Europe and Industry dataset and downscaled to the NUTS 1 level. This data was used to project grid capacity to 2036, applying historical

---

[25] JLL (2024). EMEA Data Centre Report Q4 2024. Available at: https://www.jll.com/en-uk/insights/emea-data-centre-report. McKinsey analysis estimating global demand for data centre capacity to grow by a compound average growth rate of 19% in the pessimistic scenario and 27% in the more optimistic one, with efficiency improvements, flexible workload management and supportive regulation. Available at: : https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand

[26] ICIS. Data centres: Hungry for power. Available at: https://www.icis.com/explore/resources/data-centres-hungry-for-power

CAGR trends. A validation threshold was then introduced to ensure that forecasted data centre capacity does not exceed a set share of regional power generation. This percentage was 20% for the central scenario, to reflect a situation where data centres become a relevant electricity user in line with emerging patterns in highly digitised regions; a more conservative 10% for the low scenario to reflect tighter grid constraints; while no constraints were considered for the high scenario under the assumption that major public and private investment in grid modernisation would enable substantial increases in available electrical capacity.

2.3.1.1 Scale, timing and distribution of new capacity

This section provides additional information on the scale, timing, geographic distribution and functional orientation (AI-readiness) of new data centre capacity within the EU-27 under the central growth (baseline) scenario.

Scale: the split between hyperscalers and colocation facilities is illustrated here below.

Type	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036
Colocation / CSP / telco (primary markets)	4210	5120	6068	7090	8238	9523	10577	11490	12317	13055	13703	14369
Colocation / CSP / telco (secondary markets)	2401	2921	3462	4045	4699	5433	6033	6555	7026	7447	7817	8197
Colocation / CSP / telco (developing markets)	793	965	1143	1336	1552	1794	1993	2165	2321	2460	2582	2707
Hyperscaler	5036	6125	7258	8481	9854	11391	12651	13744	14734	15615	16391	17187
	12440	**15131**	**17932**	**20953**	**24343**	**28141**	**31254**	**33954**	**36398**	**38577**	**40492**	**42460**

AI-readiness: based on the results of the CATI survey, the study estimated that in 2025 approximately 12% of total EU-27 data centre capacity is AI-ready, defined as infrastructure capable of supporting high-density AI workloads (e.g. GPU-accelerated compute, advanced cooling, and power delivery). Survey responses indicate that hyperscale operators report a substantially higher share of AI-ready capacity than colocation providers, a finding that mirrors the scale of hyperscaler investment in advanced GPU architectures. Building on this baseline, three forward-looking scenarios for AI-ready capacity as a share of total data centre infrastructure were developed.

- Slow growth scenario: By 2036, approximately 35% of total data centre capacity is AI-ready, corresponding to an average growth rate of ~32% over the ten-year period.
- Baseline growth scenario: By 2036, approximately 64% of data centre infrastructure is AI-ready.
- Fast growth scenario: By 2036, approximately 85% of data centre infrastructure is AI-ready, directly aligned with the upper-bound expectations reported by CATI survey participants

These results were also validated through the several interviews with relevant stakeholders and two workshops organized in the context of the study.

In practice, in relation to computing capacity, the market and technical reality does not lend itself to a distinction between different types of supply with the exception of the training of large AI models. As discussed in Annex 8, the training of AI models requires large, concentrated amounts of computing power. For training, low latency is not as important as for the later stages in an AI model's lifecycle. This sets AI training facilities somehow apart. To a lesser extent, large facilities dedicated to a single client (typically hyperscalers) do not need to be in proximity to an economic centre, to the difference of colocation data centres which tend to be located next to their clients, so closer to economically active areas. The policy intervention is mostly agnostic on these considerations as the most pressing needs of data centres do not differ significantly based on their end use. One of its objectives is to create the right conditions for a faster build-out of data centres and is agnostic to their ultimate use, allowing the market to find the right balance. That is why the capacity gap presented in Annex 9 (baseline scenario) looks at total data centre capacity and does not differentiate data centre according to their use (in the colocation context, the data centre operators would not even know for which downstream purpose their clients use of the server rooms offered by the colocation provider).

2.3.1 Data centre demand growth

The estimation of data centre demand builds on three scenarios (measured in MW) identified in Technopolis et al. (2025), "Study: Cloud and AI". The analysis presents corresponding projections for data centre demand across the EU27 region based off the characteristics of three strategic scenarios (low growth, central, and high growth). These projections illustrate the potential evolution of enterprise demand over the next decade.

Table 9. Overview of low growth, baseline and high growth scenarios for data centre demand

Scenario	CAGR (2025-2036)	Key assumptions and trends
Low growth	10%	• Enterprise IT budgets grow conservatively, constrained by macroeconomic headwinds, regulatory uncertainty, and cautious capital deployment across the EU27. • IT spending as a share of enterprise turnover holds steady at around 3.1%, reflecting a cautious approach to digital transformation. Within this, spending on data centre grows more slowly than in previous years, with a CAGR of approximately 8%, a notable deceleration from the 14% observed between 2021 and 2025. • Workload growth remains relatively modest, with most enterprises focusing on efficiency gains rather than significant expansion of compute-intensive workloads. AI adoption progresses slowly, resulting in only incremental increases in processing and storage demand. • Digital policy has limited influence on demand in this scenario. Private enterprises see limited incentives or pressures to scale AI or data-driven services. The lack of cohesive policy momentum results in a focus on maintaining existing infrastructure rather than investing in new capacity to support advanced workloads.
Central growth (baseline)	13%	• Enterprise IT budgets across the EU27 continue to expand at a steady and predictable pace, reflecting a stable macroeconomic environment and a measured approach to digital transformation. • IT spending as a share of enterprise turnover increases gradually, reaching 3.7% by 2032. From 2032 onwards, this ratio stabilises, indicating a maturing digital spend profile with spend only increasing to 3.8% by 2036. Within this broader trend, investment in data centre infrastructure grows in line with the historical CAGR of 14% through to 2030, reflecting sustained demand for compute and storage infrastructure. This growth supports both the retrofitting of legacy environments and the deployment of new, AI-capable facilities, particularly in markets where cloud adoption and enterprise workloads continue to scale. From 2032 onwards, the growth rate of data centre spending decelerates, but

Scenario	CAGR (2025-2036)	Key assumptions and trends
		outlays continue to increase, sustained by lifecycle refreshes, AI-capable retrofits, compliance and resilience upgrades, and steady colocation demand • Workloads evolve steadily, with increased deployment of AI, machine learning, and data-driven services contributing to higher computational requirements. • Digital policies boost private sector demand. As governments roll out e-government services, data-sharing initiatives, and sector-specific AI guidelines, private enterprises respond by adopting initiatives which steadily drive increases in compute and storage requirements.
High growth	17%	• In the fast growth scenario, enterprise IT budgets across the EU27 rise sharply as digital infrastructure becomes a central pillar of business strategy. This acceleration is driven by the widespread deployment of AI, real-time analytics, edge computing, and data-intensive applications. Organisations across all sectors and geographies invest aggressively in next-generation infrastructure, resulting in unprecedented demand for data centre capacity. • IT spending as a share of enterprise turnover increases to 4.1% by 2033. After reaching this threshold, the share stabilises through 2036, with digital operations have become deeply embedded in business models. Within this expanded IT budget, the share allocated specifically to data centre systems grows substantially reaching 23% of total IT spending by 2035, underpinned by a CAGR of approximately 11% through to 2036. This growth supports large-scale, AI-optimised infrastructure rollouts across both traditional hubs and new emerging markets. • Workload growth is exponential, driven by generative AI, large language model training, real-time analytics, and autonomous operations with enterprises requiring significantly more computational power. • Proactive and coordinated digital policies act as a powerful enabler of private sector demand. Large-scale public investments in AI, national cloud services, and public sector digital transformation signal long-term commitment to digital growth, de-risking private sector investment. Enterprises accelerate their own AI deployment, edge computing, and data management strategies to align with evolving regulatory frameworks, increased data flows, and market expectations.

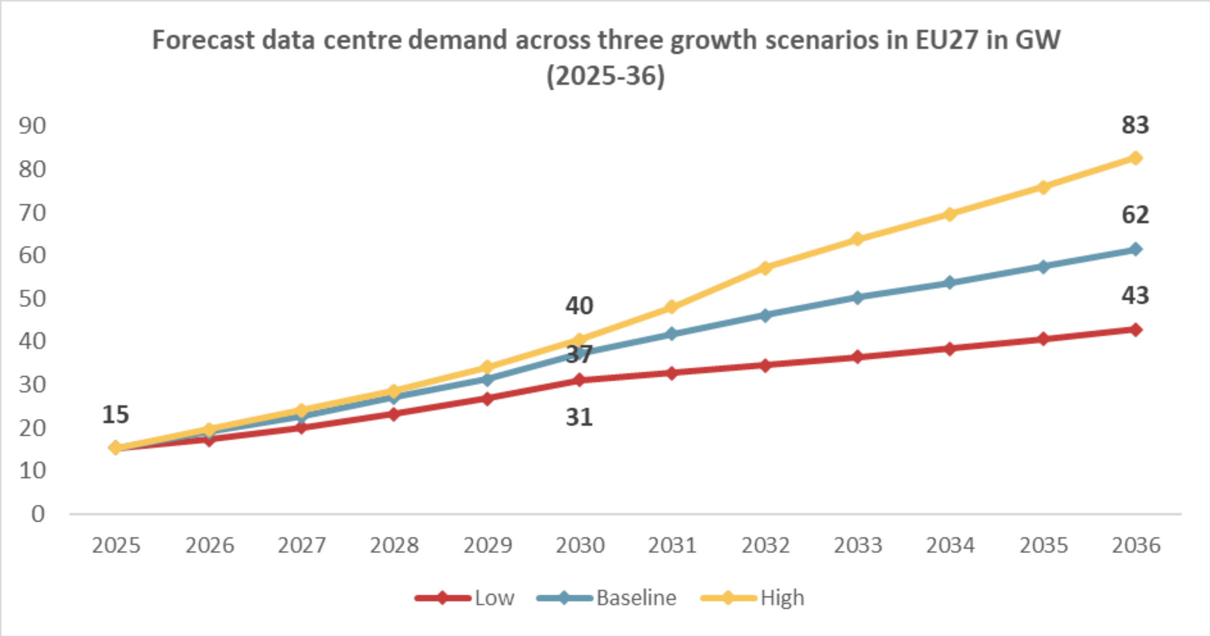
As of 2025, all three scenarios converge at an estimated 15.3 GW of installed data centre demand. However, the trajectories begin to diverge thereafter. By 2030, under the baseline scenario, demand reaches 37 GW. In the fast growth scenario, driven by increased spending, enterprise demand increases only slightly more sharply to nearly 40 GW. Meanwhile, the slow growth scenario sees more modest demand, reaching just 31 GW by the end of the decade. The

CAGR from 2025-36 for the low growth scenario is 10%, for the baseline scenario is 13% and for the high growth scenario is 17%.

Extending the demand forecast horizon to 2036 introduces greater uncertainty, reflecting the unpredictable nature of long-term market drivers, potential shifts in enterprise digital strategy, and the impact of emerging technologies such as generative AI and edge computing.

The divergence between the scenarios becomes much more pronounced. In the low growth scenario, demand reaches 43 GW, while the baseline trajectory leads to 62 GW. The fast growth scenario sees capacity expand dramatically to over 83 GW, representing a 43% increase over the central forecast and a 93% increase over our slow growth forecast.

Figure 2. Data centre demand across the EU27 in GW from 2025-36 across three growth scenarios

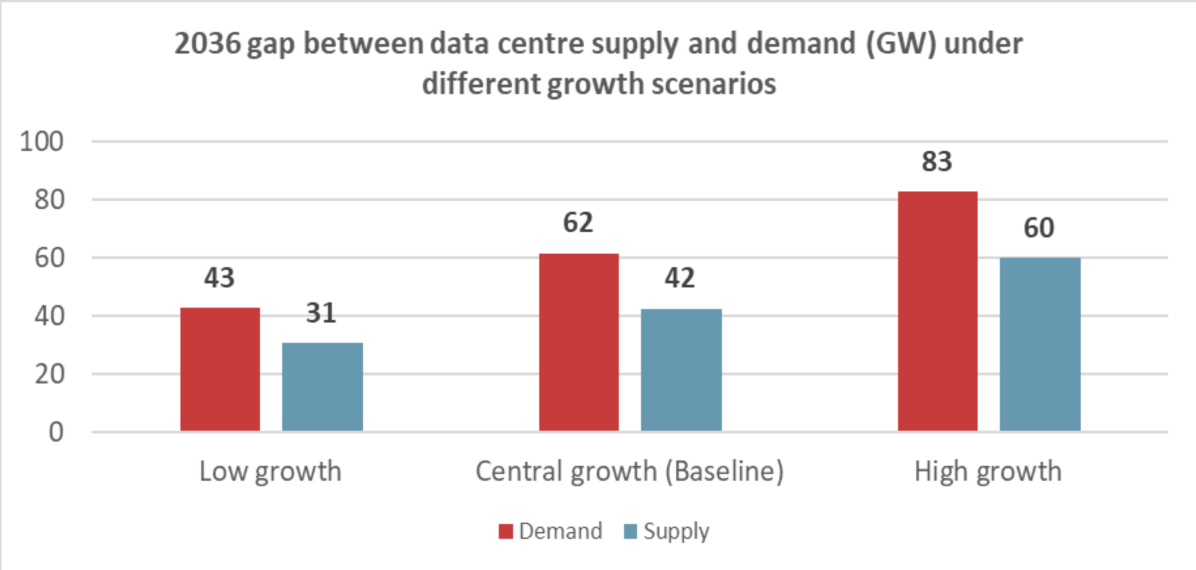


Source: Technopolis et al. (2025) by means of DataCentreMap, STL analysis

The literature aligns most closely with the status quo scenario, estimating European data centre demand at around 35 GW by 2030. In terms of growth, the study's findings are supported by global projections in the literature, which forecast a compound annual growth rate of 19% to 22% between 2023 and 2030. AI is also consistently identified as a key driver of this demand, with some sources expecting global data centre capacity to triple as a result .

Based on these projections, a supply-demand gap is expected to emerge by 2030 under all three scenarios. In the low growth scenario, the shortfall reaches approximately 7 GW, reflecting modest demand outpacing limited infrastructure expansion. Under the central trajectory (baseline), the gap widens to around 9 GW, as steady demand growth outstrips the pace of new capacity being built. In the high growth scenario, the mismatch becomes even more pronounced, with demand exceeding supply by over 13 GW, driven by accelerated adoption of AI workloads and large-scale digital infrastructure investment. By 2036 the gap becomes even more pronounced across all three of the scenarios. In the low growth scenario, the shortfall reaches approximately 12 GW, in the baseline reaches 19 GW and in the high growth it reaches 23 GW. In the high growth scenario, the gap, though still large at 23 GW, is only slightly higher than in the baseline. This is due to the assumption that rapid increases in demand are matched, at least in part, by accelerated capacity deployment enabled by more favourable investment conditions, improved regulatory agility, and large-scale public-private initiatives. However, even under this high-investment environment, the pace at which demand scales, particularly for AI and high-performance compute, still exceeds the ability of the market to deliver sufficient, AI-ready capacity.

Figure 3. Gap between data centre supply and demand in GW in 2036



Source: Technopolis et al. (2025) by means of CATI survey (n=100 companies, 280 Data Centres)

2.3.2 Data centres benefitting from each Policy Option

The analysis of policy options uses the baseline and high growth results as anchor points to estimate the impact of different policy options, with intermediate values interpolated to reflect varying scenarios and intervention intensities. Growth trajectories under the different policy options are thus modelled according to three alternative compound annual growth rate (CAGR) trends, i.e. 15%, 14% and 13%, which reflect possible deviations from the central forecast expansion path (12%). To translate capacity expansion (MW) into the number of new data centres, the following assumptions are made:

- The average data centre capacity has been derived from past deployment trends
- A forward-looking adjustment is applied, assuming an **annual increase of 1% in average data centre size**, to capture the tendency toward larger facilities over time
- For each year between 2026 and 2036, the additional MW capacity projected under the different policy growth scenarios is calculated
- The number of new data centres is then obtained by dividing the incremental annual capacity (MW) by the estimated average data centre capacity for that year.
- It is then assumed that only a percentage of new data centres each year will benefit from the policy intervention.

This approach ensures that the model accounts not only for aggregate capacity growth, but also for the evolution in average facility size, which affects how many new sites are required to deliver the expected expansion.

The tables below present the estimated number of new data centres (DC) benefitting under each policy option (PO1-A, PO1-B, PO1-C). These figures are derived by multiplying the projected number of new DCs coming online each year by the assumed percentage that would qualify for, or take advantage of, the measures under each option. The modelling distinguishes, wherever relevant, between the private market (colocation and hyperscalers) and the public sector. Enterprise data centres are not considered in the analysis.

To assess the impact of each option on data centre investment, the outcomes under each policy scenario have been compared to the baseline scenario, in which no new policy is introduced. Since the objective of each policy option is to alter investment conditions and increase data centre deployment, each scenario has been defined to reflect this potential induced build-out. To reflect uncertainty in the voluntary uptake of the mechanism, the analysis varies the share of new projects benefitting from the different policy options between 30% (low), 50% (central, reported below) and 70% (high). This range captures realistic differences in data centre facilities adoption dynamics, without assuming either full uptake or very limited benefit from each option.

Table 10. Capacity growth and new data centres under the baseline, considering no intervention
(Source: Technopolis et al. (2025))

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	CAGR
Capacity growth (MW)	12440	15131	17932	20953	24343	28141	31254	33954	36398	38577	40492	42460	**12%**
Avg. capacity of one DC (MW)	13	13.1	13.3	13.4	13.5	13.7	13.8	13.9	14.1	14.2	14.4	14.5	**1%**
No. of new DC built		205	211	226	251	278	226	194	174	153	133	**136**	

Table 11. Capacity growth and new data centres benefitting from PO1-A
(Source: Technopolis et al. (2025))

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	CAGR
Capacity growth (MW)	12440	15131	18189	21573	25409	29754	33518	36893	39965	42722	45168	47712	**13%**
Average capacity of one DC (MW)	13.0	13.1	13.3	13.4	13.5	13.7	13.8	13.9	14.1	14.2	14.4	14.5	**1%**
No. of new DC built		205	231	253	284	318	273	242	218	194	170	175	
% of DC benefitting from the option	0%	0%	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	
No. DC benefitting from the option		**0**	**12**	**25**	**43**	**64**	**68**	**73**	**76**	**78**	**77**	**88**	

Table 12. Capacity growth and new data centres benefitting from PO1-B
(Source: Technopolis et al. (2025))

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	CAGR
Capacity growth (MW)	12440	15131	18705	22839	27632	33186	38440	43409	48003	52189	55974	59991	**15%**
Average capacity of one DC (MW)	13.0	13.1	13.3	13.4	13.5	13.7	13.8	13.9	14.1	14.2	14.4	14.5	**1%**
No. of new DC built		205	269	309	354	407	381	357	326	294	264	277	
% of DC benefitting from the option	0%	0%	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	
No. DC benefitting from the option		**0**	**13**	**31**	**53**	**81**	**95**	**107**	**114**	**118**	**119**	**138**	

Table 13. Capacity growth and new data centres benefitting from PO1-C
(Source: Technopolis et al. (2025))

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	CAGR
Capacity growth (MW)	12440	15131	18447	22202	26505	31435	35912	40041	43827	47249	50315	53538	**14%**
Average capacity of one DC (MW)	13.0	13.1	13.3	13.4	13.5	13.7	13.8	13.9	14.1	14.2	14.4	14.5	**1%**

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	CAGR
No. of new DC built		205	250	280	318	361	324	296	269	241	214	222	
% of DC benefitting from the option	0%	0%	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	
No. DC benefitting from the option		**0**	**13**	**28**	**48**	**72**	**81**	**89**	**94**	**96**	**96**	**111**	

2.3.3 Impact modelling

In order to evaluate the impact of each policy option (PO1-A, PO1-B, PO1-C), a Discounted Cash Flow (DCF) model has been carried out, for a single data centre, starting at 13 MW capacity in 2025, based on the estimations calculated by Technopolis et al. (2025).

A dual approach has been used, including a company-level DCF (calculating the Weighted Average Cost of Capital (WACC) through a build-up methodology) and an external benchmarking at the MS-level (using WACC averages found in the literature for each MS[27]), to ensure that the DCF analysis is both methodologically rigorous and relevant for policymakers.

Firstly, a company level DCF has been carried out, extracting companies investing and operating data centres from Data Centre Map[28]. The following data has been extracted from companies when publicly available: WACC (if available), Cost of equity, Cost of debt, D/E ratio and beta. For private companies i.e., companies whose financial data are not publicly available, the Build-up model has been used to estimate the WACC factors.

The same analysis has been performed at the MS level, using WACC averages found in the literature. The following parameters have been gathered up or estimated for a 13 MW data centre: CAPEX, OPEX (using the energy consumption as a proxy), total revenues (fixing the expected EBITDA margin and power provisioning charged to customers has been kept in an average 165 €/kW/month[29] [30]) and corporate tax rate[31].

Energy price volatility and country-specific dynamics have been partly reflected in the model's calibration. Electricity prices used to calculate operational expenses for data centres in the discounted cash flow model have been based on non-household prices from Eurostat data and adjusted to reflect the two sourcing models identified in the CATI survey, i.e. grid supply and power purchase agreements (PPA), using a 40/60 mix. This includes declining prices driven by increasing renewable penetration, stable PPA prices for new contracts and stable network charges and non-recoverable taxes and levies. Volatility has been captured through these time-varying trajectories.

The DCF for a 13 MW project has been then performed as a European average and for each country under study, with the following assumptions:

- IT CAPEX is disbursed in two phases of 7 and 6MW capacity.
- Ramp up period: the capacity utilisation is adjusted in the first 3 years of the operations: 3 years (50% year 1, 75% year 2, 100%-year 3+).

[27] https://www.berec.europa.eu/system/files/2024-07/BoR%20(24)%20102%20BEREC_WACC%20parameters%20Report_2024_1.pdf.pdf
[28] https://www.datacentermap.com/
[29] https://www.cbre.com/insights/reports/global-data-center-trends-2025
[30] https://www.cbre.com/insights/books/european-real-estate-market-outlook-2025/data-centres
[31] https://taxsummaries.pwc.com/quick-charts/corporate-income-tax-cit-rates

- Depreciation of the construction is 15 years distributed equally while IT CAPEX presents different depreciation periods. Maintenance CAPEX has been calculated as a 3% of the total construction CAPEX yearly.
- The DCF has been presented for the first 10 years of project, using the Gordon Growth model to calculate the Terminal value (an average 2% perpetual growth rate has been considered for all countries).

As mentioned above, the WACC used has been taken from the BEREC report that uses the methodology defined by the European Commission Notice of 2019 for consistent WACC calculations across EU national regulatory authorities and supports regulatory pricing decisions in the electronic communications infrastructure sector including data centres[32].

The numbers obtained under the previous section have been used in the DCF model to estimate net benefits for data centre operators. The next present value of an average 13 MW project was calculated under the baseline scenario and under each option, varying key elements such as permitting timelines and PUE levels. The NPV difference between each policy option and the baseline was then multiplied by the number of facilities expected to benefit under each option, as derived from the possible capacity paths.

It is important to underline that the 13 MW representative data centre corresponds to the average installed capacity of data centre facilities identified in the underlying database used to construct the EU baseline. It thus reflects the observed mean of capacity distribution cross hyperscale and colocation facilities. This size is not held constant over time. As above, the average facility size is projected to increase based on observed historical trends, thus capturing the shift towards larger, capital-intensive and possibly also AI-capable facilities. It is also relevant to note that announcements of new data centres with 200 MW+ capacity are often planned and built as campus or cluster of multiple facilities implemented as smaller units, e.g. of 10 to 20 MW, that altogether compose the larger capacity, rather than a single installation.

The heterogeneity in data centres, e.g. hyperscale facilities versus colocation operators, has been incorporated into operating and financial parameters used to derive costs. Such differences were captured through PUE assumptions and utilisation rates, with hyperscalers operating at higher utilisation and lower PUEs than colocation centres on average. These parameters had a direct impact on electricity consumption and thus operating costs used in the Discounted Cash flow model. Similarly, as mentioned above, the WACC was calculated considering different business realities to reflect the different costs of capital. While any averaging compresses the dispersion, this simplification was needed in our analysis to estimate aggregate costs and benefits based on observed market dynamics and structures.

2.3.4 Energy efficiency

Starting with an average Power Usage Effectiveness, PUE, of 1.29 each policy option is expected to achieve different levels of improvement over time as shown in the figure below, with PO1-C achieving the largest impact because of the contribution of public funding to R&D and innovation in sustainable technologies.

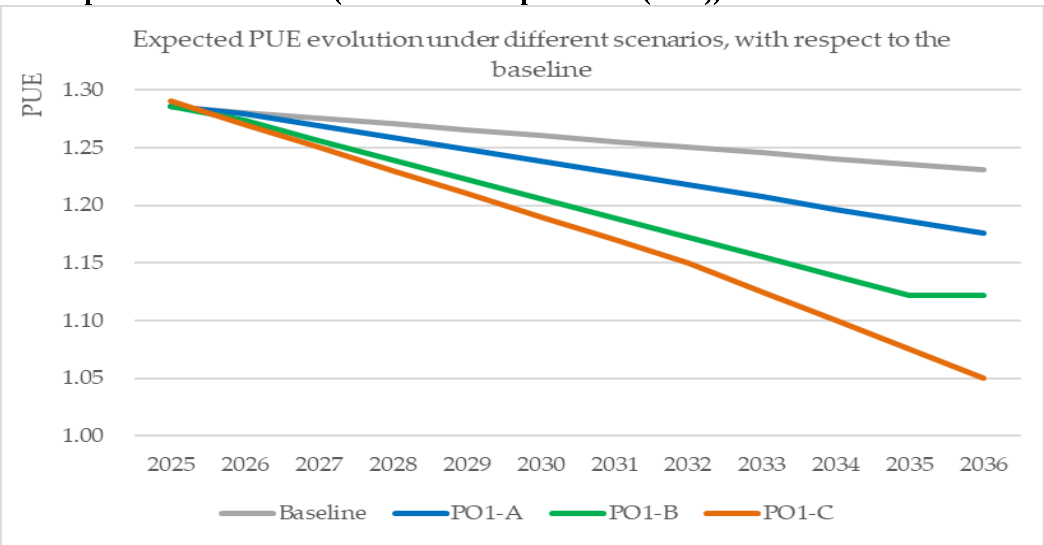
Colocation PUE was calculated using information from Data Center Map (coming out an average of 1.39) whereas hyperscaler PUE was calculated using the latest reported hyperscaler figures (coming out at an average of 1.13). The result PUE of 1.29 for 2025 is the capacity-

[32] BEREC. (2025). BEREC report on WACC parameter calculations according to the European Commission's WACC Notice of 6th November 2019 (WACC parameters Report 2025). Body of European Regulators for Electronic Communications. https://www.berec.europa.eu/en/all-documents/berec/reports/berec-report-on-wacc-parameter-calculations-according-to-the-european-commissions-wacc-notice-of-6th-november-2019-wacc-parameters-report-2025

weighted average of PUE levels identified for colocation and hyperscale facilities in the EU. This approach was used to capture the differences in efficiency across businesses of different sizes. Moreover, it has been validated with the industry during interviews and workshops, for which it was also subject to refinements and further changes as some stakeholders provided additional data on their PUE levels and market presence.

PUE improvements across the policy options are expected based on different mechanisms and time horizons. Under PO1-A, such improvements are mainly driven by the diffusion of best practices produced by the guidelines and as part of the established forum for exchanges. These are assumed to generate positive spillovers on the use of increasingly energy-efficient technologies beyond the baseline, where individual companies (usually the largest ones) have most of the incentives to invest in such technologies, without necessarily sharing the outcome of their investment. Under PO1-B, PUE reductions are driven by the stronger incentives for data centres to increase energy-efficiency due to the sustainability requirements linked to accessing the fast-track areas. These conditions are expected to increase incentives for operators to adopt higher-efficiency and sustainable solutions relatively early, as this could become a prerequisite for benefitting from accelerated permitting. Under PO1-C, in addition, data centre operators would benefit from targeted R&D programmes to optimise energy efficiency and, in some cases, deployment funds for particularly sustainable technologies and strategic uses. Since these programmes require time to develop, test and de-risk new solutions, especially for smaller operators, the most substantial PUE improvements are expected to materialise in the later years of the period. Quantitatively, this is reflected in a somewhat flatter PUE reduction in the early years and a comparatively steeper profile towards 2032–2035, when a larger share of new capacity can incorporate the mature, higher-efficiency designs.

Figure 4. Assumptions in terms of PUE improvement across the different policy options for colocation providers and public sector 2025-35 (Source: Technopolis et al. (2025))



2.4. Estimates related to Public Procurement

2.4.1 Number of public authorities procuring cloud and AI computing services

With regards to the number of public authorities that procure cloud and AI computing services and could participate at the EU-level procurement process, the assumption made is that there is one public authority in each NUTS1 and NUTS2 areas, and in most of the NUTS3 areas[33],

[33] NUTS1, NUTS2 and NUTS3 areas in Europe are close to 1,500 (https://ec.europa.eu/eurostat/web/nuts). An adjustment has been made to slightly reduce the number of NUTS3 areas with a public authority procuring cloud and AI computing services in the bigger member states where the administrative distribution at that level is more granular.

resulting in a figure of 1 206 public authorities in Europe. This figure has been confirmed when filtering the number of unique buyers of cloud and AI computing services in the procurement notices registered in the years from 2021 to 2024 at the TED portal[34] (the filtering has been done applying a search of "cloud" and "AI" strings over the TED notices with Common Procurement Vocabulary (CPV) 72 and 48). Not all public authorities launch procurement processes every year; in 2024, for instance, there were just 463 Public Administrations (PA) opening cloud and AI computing service tenders.

2.4.2 Public procurement contracts of cloud and AI computing services

The following table shows the contract award notices in EU27 by public administrations, as extracted from TED using the TED API[35]. For the ICT award notices, 'contract award notices'[36] with CPV code 72 and 48 have been considered, whereas for cloud and AI, combinations of the keywords "Cloud" or "AI" have been used as a subset of the previous. 2024 is taken as the baseline for the calculations. Then, the count of each of the results have been extracted, whereas for the share, the percentage has been calculated.

Table 14. Count of Public procurement award notices in TED for 2024. (Source: Technopolis et al. (2025), elaborated from TED data)

Count of Award Notices	2024
Cloud & AI awards	1 043
ICT awards	33 299
Share of Cloud & AI in ICT awards	3.13%
Total awards	30 7249
Share of Cloud & AI in total awards	0.34%

For the calculation of the CAGR the period spanning from 2021 – 2024 is considered. 2020 has been disregarded due to the COVID-19 pandemic effects. The values resulting from a query from TED are shown next:

Table 15. Evolution of public procurement award notices 2021 – 2024. (Source: Technopolis et al. (2025), elaborated from TED data)

Count of Award Notices	2021	2022	2023	2024	Avg 2021-2024
Cloud & AI Awards	815	915	1,017	1 043	948
ICT Awards	29 235	31 566	34 673	33 299	32 193
Total Awards	272 004	292 162	316 899	307 249	297 079
Share Cloud & AI vs Total	0.30%	0.31%	0.32%	0.34%	0.32%

The data above results in a CAGR for the period 2021 – 2024 of 8.6%. Conservatively, it is assumed that the CAGR between now and 2030 will grow at the current pace whereas it will grow half as fast afterwards.

Table 16. CAGR for public procurement award notices for ICT and cloud and AI. (Source: European Commission based on data provided by Technopolis et al. (2025))

	2021-24	2025-30	2031-36

[34] TED is the official source for public procurement in the EU. However, it is to be noted that a percentage of the data sets do not present complete information, with some fields missing.
[35] https://docs.ted.europa.eu/api/latest/index.html
[36] TED also stores the contact notices which include closed procedures with no awardees. This number is however rather small and could fall under the margin of error.

CAGR Cloud & AI Awards	8.6%	8.6%	4.3%
CAGR ICT awards	4.4%	4.4%	2.2%
CAGR Total awards	4.1%	4.1%	2.1%

With regards to the **highly critical use cases**, the assumption is that 10% of all contract award notices represent these narrowly scoped use cases[37]. Applying this to 2024 figures, the number of procurement procedures of cloud and AI computing services in that year is 52. The CAGR for this specific case is considered to be the same as for other types of use cases. The data provided in TED is not disaggregated enough to provide information on the criticality of the use cases and in some cases, the sectors are not present, making very difficult a further extrapolation.

The above assumptions yield the following projections:

Table 17. Projected number of cloud & AI awards (Source: European Commission based on data provided by Technopolis et al. (2025))

Projections	Cloud & AI Awards	Cloud & AI awards Highly critical services
2025	1 132	113
2026	1 229	123
2027	1 335	133
2028	1 449	145
2029	1 573	157
2030	1 708	171
2031	1 781	178
2032	1 858	186
2033	1 937	194
2034	2 020	202
2035	2 107	211
2036	2 197	220

An important differentiation along the document shall be the delineation between procurement tenders and bids. A tender is the procedure that a contracting authority launches while a bid is an offer that a cloud and AI computing service provider shall submit in response to the call for tender. The assumption is that as an average there are **3.5 bids** for each tender launched and awarded.

Where audit is voluntary, the assumption is that 30% of the tenders will require providers to offer an audited service, unlike when audit is mandatory, where this requirement is 100%.

The projections resulting from these assumptions are depicted next:

Table 18. Projections for the number of bids of cloud and AI computing services that need to be audited (Source: European Commission based on data provided by Technopolis et al. (2025))

[37] Member States have reported in various settings that 10% of their services fall under the category of highly critical services.

Projections	Cloud & AI bids for highly critical services (HCS) audit mechanism mandatory	Cloud & AI bids for HCS audit mechanism voluntary
2025	396	119
2026	430	129
2027	467	140
2028	507	152
2029	551	165
2030	598	179
2031	623	187
2032	650	195
2033	678	203
2034	707	212
2035	737	221
2036	769	231

2.4.3 Public procurement contract values of cloud and AI computing services

The baseline data taken into consideration for the contract values of cloud and AI computing services procured has been extracted from the TED database using the TED API[38]. To calculate the ICT contract values, the sum of the contract values of the Contract Award notices under CPV72. For cloud and AI contract values, the keywords "cloud" or "AI" have been used to discriminate.

Table 19. Public procurement contract values 2021 – 2024. (Source: Technopolis et al. (2025)) elaborated from TED data)

Value of Award notices (bn EUR)	2021	2022	2023	2024	Avg 21-24	CAGR 21-24
Cloud & AI value of award notices	2.8	5.1	12.5	9.2	7.4	48%
ICT Value of award notices	77.1	98.7	113.9	124.9	103.6	17%
Total Value of award notices	1 031.5	1 041.1	1 195.0	1 356.1	1 155.9	10%
Share of Cloud & AI in ICT awards	3.66%	5.14%	10.99%	7.38%	7.14%	26%
Share of Cloud & AI in total awards	0.27%	0.49%	1.05%	0.68%	0.64%	35%

2.4.4 Estimated number of distinct cloud and AI computing service providers in the EU

There is no common registry of cloud and AI computing service providers. Furthermore, the provision of said services is not categorized under NACE J. Under these constraints and in order to understand the current number of providers in the EU, it has been performed a desk search of Cloud Service Providers along with crossing data from various associations, market reports, TED and other documents. While this approach is limited, it has managed to capture the most relevant CSPs in the EU, both EU headquartered and non-EU.

The results of this manual search yields in the following:

[38] https://docs.ted.europa.eu/api/latest/index.html

Table 20. Number of cloud and AI computing service providers. (Source: Technopolis et al. (2025))

Cloud and AI computing service providers	Number
Total	**410**
EU-based	350
non-EU based	60

2.4.5 Audited Sovereign cloud and AI computing service providers

To calculate the number of audited sovereign cloud and AI computing service providers, the number of services listed on the FedRAMP marketplace with Impact level moderate and high[39] has been taken as baseline for the assumptions. FedRAMP is a programme that has been running since 2012 and, as of October 2025, there are currently 533 services at impact level moderate and high with the status "FedRAMP authorised" or "FedRAMP in process" or "FedRAMP ready".

The baseline situation is that in the first year, 30 cloud and AI computing service providers shall get audited, reaching up to 600 in 5 years. To reach to this number, this would imply a CAGR of 82%. The assumptions for the number of positive audits granted the first year are in line with how many authorisations FedRAMP authorised its first year of the programme, namely 2013 (10), and cross-referenced with SecNumCloud values[40].

2.5. Indirect benefits from cloud adoption

Most of the policy measures contribute to the development of European data centre infrastructure and cloud computing capacity, a richer European cloud and AI computing service offering and a more dynamic technological and industrial ecosystem, contributing to a higher adoption of cloud. This will improve the efficiency in software and IT projects, increasing productivity of IT staff, ensuring the continuity of business processes (less downtime) and facilitating migration processes. This impacts not only the efficiency of the IT staff but also the flexibility and capability of the European private and public sector to adapt in an agile way to evolving market needs and conditions, and to the dynamic technology landscape, increasing its competitiveness. This could have been measured in terms of effort saved in IT tasks (FTEs), but it would have been difficult to allocate the specific contribution of each specific measure, adding potential risk of double counting their effect. The policy measures related to federation and joint procurement are making the biggest contributions, while most of the others will have a more limited impact.

Cloud computing services generally offer a significant number of benefits, among them also the drive or productivity. The OECD reports strong productivity effects through cloud software investment, especially for low productivity firms, suggesting that such companies derive greater productivity benefits from this investment when fixed costs are lower and scaling-up opportunities are higher. It is implied that cloud adoption has the potential to support the

[39] https://marketplace.fedramp.gov/products

[40] Source: https://cyber.gouv.fr/sites/default/files/document/catalogue-produits-services-qualifies-agrees-certifies-anssi_0.pdf . The list of services qualified are listed in Chapter 5.1. This table shows 9 individual cloud service providers qualified but 16 cloud services with the following breakdown: 2 services in 2023, 2 services in 2024 and 12 in 2025.

productivity catch up of latecomer firms, while low cloud adoption could still hamper broader productivity gains[41].

3. IMPACTS OF POLICY MEASURES IN TERMS OF COSTS AND BENEFITS

The assumptions presented below and used for the estimation of the impacts of policy measures on key stakeholders draw on recognised literature sources and observable practices in the industry and the public sector. To test their robustness, the supporting study led by Technopolis conducted a series of one-to-one interviews with a diverse set of relevant stakeholders. These assumptions were further scrutinised in the study's final validation workshop, which led to an adjustment of some parameters.

3.1. PM1: Expanding the Alliance for Industrial Data, Edge and Cloud with a working group on data centres and extending membership to relevant players

Under this measure, the European Commission would set up an additional Working Group (WG) under the Alliance for Industrial Data, Edge and Cloud to include data centre operators. This would facilitate the exchange of best practices on the deployment of data centres with the objective to foster EU-located capacity, while collectively addressing the obstacles that hold back data centre investment and expansion in the EU.

Impact on data centre deployment acceleration. This new working group may improve deployment speed for the participating alliance members. The reduction in data centre deployment time will likely be very slow due to the limited reach of the initiative, the time required to produce and disseminate results, and the lack of structural effects.

Adjustment costs for data centre operators. Participation in the new working group is voluntary at entry but implies expectations of active attendance and contribution once membership is granted. This is expected to generate adjustment costs for stakeholders willing to participate. Under the Better Regulation Toolbox, these can be considered consultation-related burdens, although voluntary. Thus, the recurring source of adjustment costs for data centre operators arises from their involvement in the newly established Working Group, who would face additional costs for travel and participation in this new structure. This is based on 2.5 days of effort per participant for each in-person meeting (i.e. 1 day of attendance and 1.5 days of preparation), assuming two General Assemblies (in-person meetings) per year. In addition, participation in 10 webinars annually has been costed at 0.5 days of effort (or 4 hours) per participant per webinar, including both attendance and preparatory work. Please see the formula below. These are estimated at approximately EUR 5,400 per operator each year, made up of EUR 2 000 for in person engagement, EUR 2 000 for webinar participation and EUR 1 400 for travel expenses (estimated at EUR 700 per trip per participant). The Working Group is expected to involve 30 new delegates: therefore, the total recurrent adjustment cost stems from multiplying this total per participant by 30 and discounting it at present value.

$$\textit{Recurrent adjustment cost}_{\textit{per participant,year}} = (\textit{Days per in-person meeting} \times \textit{No. of in-person meetings} \times \textit{labour cost}) + (\textit{Travel cost} \times \textit{No. of in-person meetings}) + (\textit{Days per webinar} \times \textit{No. of webinars} \times \textit{Labour costs})$$

[41] OECD Compendium of Productivity Indicators 2025

Additional effort has been considered for around 40% of the Working Group members, who would be active in producing documents, i.e. roadmaps or reports, each year, estimated at around 20 days of additional work per year, for a total of EUR 96 008 each year. This estimate reflects the contribution of the chairing team and rapporteurs, elected from within the WG, who are responsible for supporting and implementing the group's daily activities. Although not mandatory, these recurrent activities would be undertaken in the operators' best interest to gain information and reduce uncertainty in project development. For this, the formula is:

$$\textit{Document production}_{\textit{40\% subgroup/year}} = (40\% \times \textit{Total No. of participants}) \times (\textit{Effort of active engagement} \times \textit{labour cost})$$

Total recurrent adjustment costs for data centre operators under PM1 are thus estimated at EUR 2.2 m (NPV, 10-years).

Cost savings for data centre operators. The cost savings for data centre operators are explained as indirect impacts as the reach of this measure is by design not enough to justify a monetisation.

No new costs or cost savings have been considered for national public authorities, as they would not participate in this new Working Group and are already participating in the General Assembly (as members of the Member State Cloud Cooperation Group), to which this new working group would report.

Administrative costs for the European Commission. The establishment and onboarding of the new Working Group entails one-off administrative costs for the Commission. The related costs are estimated considering the time taken to onboard the new delegates in the Working Group during the first year, considering 20 days or 0.09 FTE-year in 2027. This would be facilitated by the existence of an existing working group of cloud and edge providers [42]. Recurrent costs would reflect the additional administrative costs linked to the coordination of the new Alliance WG, i.e. preparing the work programme, meeting planning, agenda-setting, inviting stakeholders, circulating minutes, drafting reports, managing documents, dealing with day-to-day queries, running webinars and preparing them, for which 40 days per year have been considered. These would include the additional meetings per year, preparation and reporting towards the Alliance Members. Total administrative costs have been calculated as the one-off administrative costs in year 1 plus the discounted value of the recurrent annual administrative costs over 10 years.

$$\textit{Total administrative costs} = \textit{one-off administrative costs} + \textit{recurrent administrative costs}$$

$$= (\Delta T \times \textit{labour cost})_{\textit{year 1}} + \sum_{t=2}^{10} \frac{(\Delta T \times labour\ cost)_{year\ t}}{(1+0.03)^{t-1}}$$

Total (one-off and recurrent) administrative costs for the Commission under PM1 are thus estimated at EUR 0.1 m (NPV, 10-years).

Indirect impact: The WG will help to foster EU-located capacity, providing advice, guidelines and recommendations to remove or reduce the obstacles that hold back data centre investment and expansion in the EU. This contribution will help the European Commission and national public authorities (NPAs) to orient their policies and data centre operators to fine tune their deployment plans. However, it is also possible that larger companies will be willing to invest

[42] Assumptions behind these numbers have been validated with EC staff currently working on the Alliance for Industrial Data, Edge and Cloud.

more time and resources into the participation compared to SMEs, and that the measure will be more costly in relative terms for SMEs – despite this is hard to quantify.

Sensitivity analysis: No sensitivity analysis has been conducted on this policy measure as the amounts at stake are too small.

Results: For PM1, the estimated costs for the implementation of this measure across all stakeholders are EUR 2 339 297. These costs reflect the recurrent administrative costs borne by the additional Commission staff for the ongoing coordination, meeting and time to manage the working group activities (EUR 130 696). On top of these, a small one-off administrative cost (EUR 7 661) is foreseen for initial setup tasks. The measure also includes the adjustment costs expected to be incurred by data centre operators and CSPs from participating in the WG.

Table 21. Expanding the Alliance for Industrial Data, Edge and Cloud with a workgroup on data centres and extending membership to relevant players (PM1)

Cost types	Data centre operators (€)	Public authorities (€)	European Commission (€)	Total Value (central, €)	Total Value (min, €)	Total Value (max, €)
one-off administrative	-	-	7 661	7 661	7 661	7 661
recurrent administrative	-	-	130 696	130 696	130 696	130 696
one-off adjustment	-	-	-	-	-	-
recurrent adjustment	2 200 940	-	-	2 200 940	2 200 940	2 200 940
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	2 200 940	-	138 357	2 339 297	2 339 297	2 339 297
Total benefits	-	-		-	-	-
Net impact	**2 200 940**	-	**138 357**	**2 339 297**	**2 339 297**	**2 339 297**

3.2. PM2: Creating a forum for exchanges between relevant public and private stakeholders involved in the buildout of data centres

Under this measure, the Commission would establish a dedicated forum to facilitate structured exchanges between the key public and private stakeholders involved in the deployment of data centres, with the objective of accelerating the deployment of innovative and sustainable capacity in the EU. These fora would provide a structured platform for dialogue and coordination, enabling shareholders to share knowledge, identify challenges and coordinate approaches across the different stages of data centre planning, construction and operations. The forum would bring together all relevant actors, including transmission system operators (TSOs), connectivity providers, data centre operators, equipment manufacturers, and local and regional authorities. The purpose of the forum would be to support the uptake of advanced and sustainable technologies that can increase capacity while reducing the environmental footprint of data centres and to identify and address the obstacles currently hindering investment and expansion. These exchanges would also allow to include discussions on the needed communication regarding the trade-offs, benefits and potential mitigation strategies for public contestation of data centres. By fostering early and continuous exchanges, the forum would enable stakeholders to align on technical requirements, investment priorities, and regulatory expectations.

Impact on data centre deployment acceleration. This forum is expected to contribute to creating a more predictable and investment-friendly environment for data centre deployment, supporting the EU's objectives of technological leadership, strategic autonomy, and sustainable digital infrastructure growth. This is expected to increase efficiencies in the deployment of a number of new data centres, especially of those operators participating in the forum. This would be the consequence of increased exchanges of best practices, and reduced interactions between economic operators and authorities.

Adjustment costs for data centre operators. Recurrent participation in newly established fora is classified as a recurrent adjustment cost for organisations choosing to participate on an ongoing basis and are expected to contribute actively once involved, i.e. in terms of resource commitments associated with meetings, preparation and coordination. Assuming two in-person events per year and five online webinars per year, the participation requirement amounts to approximately 7.5 staff-days per participant per year, plus travel costs per in-person trip. Participation is expected from 30 data centre operators and 10 CSPs active in the deployment of data centres, reflecting the forum’s focus on data-centre deployment issues. The cost for other private sector stakeholders is not factored.

Total adjustment costs for data centre operators under PM2 are thus estimated at EUR 1.5 m (NPV, 10-years)

Cost savings for data centre operators. The cost savings for data centre operators are described as indirect costs as the magnitude and reach of the measure is by design not big enough for these costs to be monetised.

Adjustment costs for national public authorities. Recurrent adjustment costs for public authorities are primarily linked to their participation in the exchanges. For simplicity, it is assumed that 27 national authorities take part each year, although in practice representation may also be delegated to local authorities, depending on their involvement in data centre deployment. These costs cover attendance and preparation for two in-person meetings annually, as well as participation in a programme of five webinars per year for each authority.

Total recurrent adjustment costs for national public authorities under PM2 are thus estimated at EUR 0.8 m (NPV, 10-years).

Recurrent savings for national public authorities. The cost savings for public authorities are described as indirect costs as the magnitude and reach of the measure is by design not big enough for these costs to be monetised.

Administrative costs for the European Commission. The Commission would incur one-off administrative costs to organise the exchanges, covering tasks such as defining the rules of procedure, issuing invitations and setting up the platforms for interaction. These start-up costs are estimated at approximately 40 staff days (equivalent to 0.2 FTE) for the first year of operation. Recurrent costs would arise from the supervisory and organisational role of the Commission in managing the forum. This is estimated at 40 staff days annually (0.2 FTE) for coordination and oversight, including the time dedicated to organising and participating in two in person events and five webinars per year. Furthermore, the cost of hosting one in-person event per year at the Commission’s premises is estimated at EUR 5 000.

Total administrative costs (one-off and recurrent) for the Commission under PM2 are thus estimated at EUR 0.2 m (NPV, 10-years)

Indirect impact: For data centre operators cost savings under this measure would stem from coordination efficiencies due to these discussions focused on data centre development across the EU. The forum is expected to reduce duplicated outreach and bilateral exchanges with key stakeholders, such as permitting authorities, TSOs and local administrations when building new data centres.

Recurrent cost savings for national public authorities are expected from the centralisation of exchanges through the forum, which reduces repeated bilateral interactions with providers.

Sensitivity analysis: As above, no sensitivity analysis has been conducted on this policy measure as the amounts at stake are too small.

Results: For PM2, the estimated net costs for the implementation of this measure are EUR 2 603 530. These stem mostly from recurrent adjustment costs (EUR 2 372 210) stemming from the participation in the forum by the national public authorities and the economic operators. A one-off administrative cost (EUR 15 322) is foreseen for initial setup tasks borne by the Commission. Recurrent administrative costs of 215 998 are foreseen in relation to coordination for the management of the forum discussions. No direct savings are expected.

Table 22. Creating a forum for exchanges between relevant public and private stakeholders involved in the buildout of data centres (PM2)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	15 322	15 322	15 322	15 322
recurrent administrative	-	-	215 998	215 998	215 998	215 998
one-off adjustment	-	-	-	-	-	-
recurrent adjustment	1 553 531	818 679	-	2 372 210	2 372 210	2 372 210
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	1 553 531	818 679	231 320	2 603 530	2 603 530	2 603 530
Total benefits	-	-	-	-	-	-
Net impact	**1 553 531**	**818 679**	**231 320**	**2 603 530**	**2 603 530**	**2 603 530**

3.3. PM3: Adopting guidelines on building sustainable data centres in the EU

Under this measure, the Commission would develop non-binding EU guidelines for the sustainable planning, design and operation/deployment of data centres, which complement existing initiatives, e.g. DG ENER's grid package, the EED, and the simplification of environmental permitting. The guidelines would prioritise voluntary coordination over top-down prescription. Their purpose is to address practical bottlenecks encountered by market participants and national public authorities, notably in terms of permitting, grid access, and financing, while promoting the uptake of innovative and resource-efficient technologies. They would also include recommendations on identifying suitable areas for data centre deployment. The guidelines would be co-created with Member States, relevant regulators, local authorities, TSOs/DSOs, data centre operators and CSPs. Drafting would also draw on the forum established under PM2, public consultations, and periodic review to reflect technological progress and implementation feedback. The text would be adaptable to national or regional contexts, allowing authorities to reference it if consistent and helpful with respect to domestic frameworks.

Governance cadence. Initial issuance of the guidelines in 2027, followed by triennial reviews (2030, 2033, 2036) to reflect technological progress and implementation feedback.

Impact on data centre deployment acceleration. The baseline capacity growth presents a 12% CAGR in data centre capacity (2025-2036). Under this option, it is assumed that the capacity growth rate (CAGR) increases slightly to 13% (see section 2.3.1 of this Annex). The guidelines are expected to reduce design, assessment and administrative tasks and applying best practices in datacentre rollout and operation. The scope of this measure covers data centre operators and CSPs active in the building of data centres in the EU. Impacts scale with the share of organisations adopting the guidelines and the share of new projects applying them (see section 2.3.3). Since the use of the guidelines is voluntary, it is assumed that the share of new projects applying the guidelines increases from 0% in 2027 to 50% by 2036, to consider the differing views received during the consultations of Technopolis et al. (2025) about the usefulness and rate of uptake of the guidelines.

Adjustment costs for data centre operators. The impact of the guidelines on businesses is modelled as adjustment costs using the Standard Cost Model (SCM), which accounts for the time and resources needed to understand and apply the guidelines. In year 1, each participating operator incurs one-off adjustment costs for consultation and discussions of the guidelines with authorities. Participation in the initial consultation process is estimated for 30 data centre operators and 10 CSPs[43], considering around 27.5 staff days per operator per year (equivalent to 0.125 FTE or around 2-3 full working days per month, spread across the year)[44]. The continued involvement in the revisions/updates of the guidelines is estimated at an additional 20 days every three years, but only for the 30 data centre operators and 10 CSPs originally engaged in the drafting. These days of effort per operator for participating in the discussion of the guidelines every three years and until 2036 would entail adjustment costs of EUR 1.58 m in total (NPV), assuming 30 data centre operators and 10 CSPs.

For operators adopting the guidelines, 20 days per operator are considered for checking/adjusting planned solutions for the roll-out of data centres or of existing processes. It is assumed, backed by the results of the Final Workshop of the study carried out by Technopolis et al. (2025), that 50% of the approximately 400 CSPs and data centre operators active in building data centres in the EU would adopt the guidelines and adjust their processes. Consequently, adjustment costs are estimated to amount to around EUR 29 317 per operator.

Total adjustment costs (one-off and recurrent) for data centre operators under PM3 are thus estimated at EUR 7.4 m (NPV, 10-years)

Administrative cost savings for data centre operators. The benefits generated by voluntary guidelines, e.g. fewer mistakes, reduced rework, faster processes and improved coordination, are classified as administrative burden reductions. The impact of the guidelines is modelled by assuming shorter administrative timelines using a SCM approach. The guidelines are expected to reduce the incidence of mistakes during the pre-operation phase of building a new data centre. This is modelled as a central 10-days saving (min 5 days; max 15 days), with an increasing number of data centres benefitting from this measure (subject to sensitivity analysis). The time saving benefit of the voluntary guidelines is calculated as the time saved per facility that adopts the guidelines (ΔT) multiplied by the relevant labour cost, the total number of new facilities, and the estimated adoption rate. This follows the SCM formula:

[43] The number of operators engaging with the drafting of the guidelines represents the average number of operators typically engaging in such processes, i.e. not the total number of operators in the EU.

[44] Although this consultation is voluntary and not a legal obligation, operators are likely to engage due to their interest in influencing a framework that directly affects their operations

$$\text{Total savings} = \Delta T \times \text{labour cost} \times s \times \text{No. new facilities}$$

Total administrative cost savings for data centre operators under PM3 are thus estimated at EUR 2.1 m (NPV, 10-years)

Adjustment costs for national public authorities. For public authorities that participate in drafting the guidelines, adjustment costs would be related to their participation in the drafting of the guidelines and their internal adoption, in terms of familiarisation and optional adaptation of local checklists and templates, estimated at 30.5 days per year (0.14 FTE) or around 2-3 days per month of full-time work per national authority spread across the year of adoption. If one representative from each Member State would participate, this would translate into approximately EUR 236 575 in year 1. Thereafter, adaptation of the new templates/tools together with the participation of authorities in the review of the guidelines every three years are expected to require 20 staff days (0.1 FTE). This would entail recurrent adjustment costs of EUR 155,131 each update cycle, assuming all Member States would adopt the guidelines.

Total recurrent adjustment costs for national public authorities under PM3 are thus estimated at EUR 0.6 m (NPV, 10-years)

Administrative cost savings for national public authorities. Harmonised EU guidelines are expected to limit the need for national authorities to interpret divergent compliance questions during permitting. Authorities are expected to realise administrative burden reduction once the guidelines are applied, including reduced errors, faster processing with fewer clarifications, and improved coordination with operators. These time and resource savings are counted as administrative cost savings in the impact assessment and are quantified using Standard Cost Model principles. From 2027 onwards, clearer information requirements are assumed to generate lasting process efficiencies, reducing administrative efforts per project and lowering disputes with data centre operators, as well as the need for repeated iterations with applicants. Given that operators are expected to save 10 days per project, a proportional reduction of approximately 20% on the authority side is applied, resulting in an estimated saving of 2 days (min 1 day; max 3 days) per project (ΔT). This reflects reduced requests for clarification, fewer iterative corrections and smoother coordination thanks to the guidelines. The savings would largely depend on the voluntary adoption of the guidelines by the new data centre projects, allowing authorities to save time in terms of decreased interactions with them. Benefits are estimated considering they would accrue to around 50% of national public authorities (central estimate) in the EU dealing with data centre projects.

$$\text{Cost savings}_{PA} = \Delta T \times \text{labour cost} \times s \times \frac{No.new\ facilities}{MS} \times \text{No of MS}$$

Total administrative cost savings for national public authorities under PM3 are thus estimated at EUR 0.3 m (NPV, 10-years)

Adjustment costs for the European Commission. The Commission would be in charge of developing the guidelines, requiring one-off adjustment costs covering the drafting, consultation, translation and dissemination. These tasks are estimated to require around 110 staff days during the first year (0.5 FTE). Thereafter, periodic improvements and reviews, comprising an update every three years, would require about 55 staff days (0.25 FTE) for each update cycle.

$$\text{Total adjustment costs} = \text{one-off adjustment costs} + \text{recurrent adjustment costs} = (\Delta T \times \text{labour cost})_{year\ 1} + (\Delta T \times \text{labour cost})_{year\ update}$$

Total adjustment costs for the European Commission under PM3 are thus estimated at EUR 0.1 m (NPV, 10-years)

Indirect impact: The guidelines are supposed to support cross-fertilisation of best practices, especially for those operators with operations across EU27 borders, and by doing that they should work towards the improvement of the investment climate for green and sustainable technologies for data centres rollout.

Sensitivity analysis: The key parameters tested for sensitivity include (1) the adoption rate of the guidelines in terms of the number of projects concerned, (2) time saved per project for operators and authorities. For such purposes min-max were created for these parameters. The number of projects benefitting from the guidelines ranges from 30% in the low scenario to 70% in the high scenario, with a central estimate of 50%. A low case combines a conservative adoption rate and limited time savings, while a high case combines a high adoption rate with higher efficiency gains.

Results: The table below presents the aggregated costs for all stakeholders for the implementation of this measure. Total implementation costs are estimated between EUR 4 948 939 to EUR 15 841 158, while total cost savings range from EUR 1 298 171 to EUR 4 191 108, with a central value of EUR 2 383 022. The measure is therefore costly in all cases. The min and max scenarios are largely driven by the adjustment costs required and consequent cost savings expected.

Table 23. Creating guidelines on building sustainable data centres in the EU (PM3)

Cost types	Data centre operators	Public authorities	European Commission	Total Value (central, €)	Total Value (min, €)	Total Value (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-	-	-	-	-	-
one-off adjustment	2 080 146	-	40 907	2 121 053	1 305 468	4 159 557
recurrent adjustment	5 363 245	612 097	51 523	6 026 866	3 653 471	11 681 301
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	7 443 391	612 097	92 431	8 147 919	4 948 939	15 841 158
Total benefits	(2 103 643)	(279 379)	-	(2 383 022)	(1 298 171)	(4 191 108)
Net impact	**5 339 748**	**332 718**	**92 431**	**5 768 775**	**3 650 768**	**11 650 050**

3.4. PM4: Project facilitators for the roll-out of data centres

Under this measure, Member States would simplify the administrative efforts required to roll out data centres, by designating a project facilitator acting as a central coordinator for the permitting process at national level, where this does not already exist. Member States would be free of designating the facilitator as per their own structures, e.g. a service within their central administration or within an agency. The project facilitator would be responsible for accompanying the applicants in securing all relevant authorisations (including environmental assessments, construction permits and/or grid connection permits) and coordinating with other national agencies/administrative entities (e.g. possible future single points of contact for environmental assessments) involved in the permitting process on one side, and with the data centres on the other. It would also provide support to the data centre operators in assessing whether projects qualify to be recognised as strategic, thereby enabling them to benefit from access to funding, helping data centres demonstrating readiness when it comes to grid connection, and dedicated administrative support. For environmental authorisations, the project facilitator would interact directly with the designated authorities or through the national single point of contact (SPOC), ensuring that there is efficient coordination.

Evidence from Technopolis et al. (2025) covering 12 Member shows that overall permitting timelines, i.e. including zoning & land allocation, building permit, utilities & grid connection, environmental permit/s currently range 32 months on average (see section 98 of this Annex for a more detailed overview).

Impact on data centre deployment acceleration. The baseline capacity growth presents a 12% CAGR in data centre capacity (2025-2036). Under this option, it is assumed that the capacity growth rate increases to 15%. This uplift reflects the assumption that shorter, more predictable permitting procedures reduce barriers to investment, accelerate time to market, and improve certainty for operators, thereby stimulating additional capacity deployment. The scope of this measure covers data centre operators and CSPs active in new data centre builds in the EU (see section 2.3 of this annex for further details). It is assumed that 50% of the new builds will be adopting this measure, in a staged adoption going from 0% in 2027 until 50% in 2036. This is a conservative assumption used for modelling purposes only, with the caveat that the detailed assumptions of number of new builds forecasted per country per year is not considered, and not knowing how many countries will adopt this measure.

Costs for data centre operators. Data centre operators will engage with the facilitator to submit necessary documents, attend joint meetings and receive guidance on the permitting processes. From the operator's perspective this should replace the numerous, fragmented integrations with individual authorities that currently occur, resulting in limited additional costs. Although operators may incur some initial costs to familiarise themselves with the facilitator's procedures, these are likely to be outweighed by benefits in terms of fewer repeated submissions and shorter procedures (see below). As the measure is expected to simplify the process without increasing the overall time spent on permitting, no separate administrative cost is considered for data centre operators.

Direct economic benefits for data centre operators. The most relevant benefits of this measure arise from the direct economic benefits of earlier cash-flow realisation for one project linked to shorter permitting times achieved through the accompanying effects of the facilitator, i.e. the reduction in administrative processing time and the resulting acceleration of the overall development timeline for new data centre projects[45]. These benefits represent a subset of all the potential improvements generated by the measure, but they are the ones that can be robustly monetised. To capture them, the analysis applies a project-level Net Present Value (NPV) approach (discounted cash flow) that compares the baseline permitting duration with the accelerated scenario and measures the economic value of bringing construction and commercial operations forward, discounted at the project WACC (6%). Earlier time-to-market gains from faster permitting are reflected directly in the DCF through a shorter period before revenues are realised and thus earlier start of cash flows, while reduced operating costs from improved energy efficiency (declining PUE, baseline scenario) are included as part of the OPEX assumptions over the life of the project. Risk-related efficiency gains, e.g. better certainty on

[45] Although all parameters (PUE, utilisation rate, revenues and costs) are held constant between the baseline and this policy scenario, the discounted cash-flow model is inherently non-linear in time. Therefore, shortening the permitting phase brings forward the entire operating cash-flow profile, reducing discounting on the most value-relevant early-operation cash flows.

siting, permitting and investment conditions, are considered indirect benefits rather than appearing directly in the model[46].

The simplified process through the use of a project facilitator is estimated, based on interviews with stakeholders and validated during the final validation workshop, to shorten the average permitting duration for a new data centre facility by 6 months, from an average baseline of 32 months to around 26 months duration from the development phase to operations. The NPV gain associated with this reduction in permitting timelines is not driven only by timing effects. The project's cash-flow model incorporates several operational and financial parameters that together increase the economic value of accelerated deployment, resulting in a higher NPV than would be obtained through time-shifting alone. Consequently, the NPV increase from EUR 58 million to EUR 65 million reflects the combined impact of accelerated commissioning and improved operational performance, which contribute to the economic benefit of permitting simplification.

$$\textit{Direct economic benefit} = \Delta NPV = NPV_{PM4} - NPV_{baseline}$$

Where each NPV is computed over a 10-year horizon and includes all cash flows: CAPEX outflows during construction, OPEX, Revenues. The analysis has been carried out in nominal terms, with both costs and revenues indexed over time and discounted using a nominal WACC.

NPV baseline (EUR m)	58.32	**Economic benefits per project (EUR m) Timeline reduction of 6 months**	
NPV after PM implementation (EUR m)	64.74	6.42	11%

Beyond the quantified impact, the measure is also expected to generate additional direct benefits such as improved information for operators and authorities, reduced administrative friction, and greater market efficiency through more consistent and predictable interactions with permitting bodies. These impacts can be considered administrative cost savings, improved information and better market efficiency, under the Better Regulation. They are not monetised because of their smaller scale compared to the efficiency gains captured through the NPV differences.

Total direct economic benefits for data centre operators under PM4 are thus estimated at EUR 4.6 bn (NPV, 10-years)

Adjustment and enforcement costs for national public authorities. National authorities are expected to face one-off adjustment costs to comply with this measure and establish the project facilitator. These costs arise to design and implement streamlined permitting procedures, designate and staff a task force and align responsibilities across relevant authorities. For modelling, a one-off cost of around EUR 0.4 million per Member State has been assumed to capture the effort to (i) set up the project facilitator, i.e. defining the mandate, governance, allocation of responsibilities and decisions (1 FTE), (ii) staff new people, i.e. initial team preparation and training (2 FTEs), (iii) design streamlined procedures and guidelines (1 FTE) and (iv) coordinate effectively among different authorities, i.e. meet with relevant ministries, agencies, authorities and other bodies, as well as secretariat support (2 FTEs). This cost corresponds to a total effort of 6 FTEs to enable the measure's organisational design, workflow streamlining, initial staffing and coordination with other authorities. To reflect differences in territorial complexity and the number of administrative regions involved, this amount has been

[46] The same applies to other measures using this modelling approach, i.e. PM5 and PM10.

uplifted with a mark-up for each NUTS administrative tier (NUTS 1/2/3), i.e. + EUR 0.052m per NUTS-1 region, + EUR 0.01m per NUTS-2 region, + EUR 0.005 m per NUTS-3 region[47].

The measure would also entail recurrent enforcement costs for national authorities, reflecting the operations of the project facilitator and task force once established. These include staff time for coordinating with competent authorities, handling applications, maintaining harmonised workflows and acting as a central interface for data centre projects. These costs are mainly staff-time-based, assuming 4 FTEs/year. The total EU-wide costs are obtained by multiplying Member State–level savings by the total number of Member States.

Total costs (one-off adjustment and recurrent enforcement) for national public authorities under PM4 are thus estimated at EUR 78.9 m (NPV, 10-years).

It is important to underline that 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.

Administrative cost savings for national public authorities. Recurrent savings for national public authorities should stem from administrative simplifications given the assumed reduction of parallel processing and fewer back-and-forth interactions between authorities and with economic operators. In the baseline, permit applications are processed through multiple parallel channels, with each authority devoting staff time to separate contacts, repeated information requests and uncoordinated reviews. Under the new set-up, a dedicated facilitator team would coordinate input, standardise documentation and organise joint meetings. As a result, and based on the interviews conducted, the total number of staff days required per project across all authorities is assumed to decrease, even though some of this effort is reallocated. The figures used consider that average processing of permitting procedures currently requires around 80 staff days (or 20 weeks) per project by each authority. Under the measure, process redesign and single-window coordination could reduce this by approximately 20 staff days per new data centre project (15-25 for sensitivity).

$$\text{Cost savings}_{PA} = \Delta T \times \text{labour cost} \times s \times \text{No. new projects} \times \text{No. of MS}$$

Total administrative cost savings for national public authorities under PM4 are thus estimated at EUR 110.8 m (NPV, 10-years)

Indirect impact: This measure is also expected to produce wider economic benefits and non-monetary benefits, such as reduced investment uncertainty, more predictable project planning, lower likelihood of disputes or appeals, enhanced coordination across authorities, and a more attractive investment environment for large-scale digital infrastructure. While these indirect effects are not quantified, they reinforce the overall positive impact of the measure and help explain the broader efficiency gains supported by the quantified analysis.

Sensitivity analysis: Four key parameters are subject to sensitivity checks because of the complexity of this policy measure and the number of assumptions implied most affecting the balance of costs and benefits. The parameters subject to sensitivity are: (i) the time saved in

[47] NUTS counts proxy multi-tier coordination and interface complexity (more NUTS-levels/regions implies small regions. The EU currently lists 92 (NUTS-1), 244 (NUTS-2), 1,165 (NUTS-3) regions, underscoring the heterogeneity across Member States.

permitting processes (ΔT) as this determines the scale of the economic benefits for operators through time-to-market acceleration (varied between 4 and 8 months), (ii) the number of data centre projects that would benefit by 2036, (iii) the implementation costs for authorities and (iv) time savings for permitting by public administrations. These dimensions form the low and high scenarios to test potential outcomes of this measure.

Results: The aggregated costs and benefits for all stakeholders over the time horizon are summarised in the table below. While operators do not incur additional direct and experience substantial economic benefits from time-to-market acceleration, national public authorities face one-off adjustment and recurrent enforcement costs, with administrative cost savings from simplification. Even though authorities' cost savings slightly outweigh their costs in all scenarios, the large economic benefits accruing to operators dominate the overall balance. The differences between scenarios are mainly driven by changes in the magnitude of the NPV gains linked to the expected reduction in permitting timelines.

Table 24. Administrative simplification for the roll-out of data centres (PM4)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-		-	-	-	-
one-off adjustment		20 668 601	-	20 668 601	19 011 860	22 325 342
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	58 225 227	-	58 225 227	29 112 613	87 337 840
Total costs	-	78 893 828	-	78 893 828	48 124 473	109 663 182
Total benefits	(4 585 666 446)	(110 843 709)	-	(4 696 510 155)	(1 908 005 277)	(8 742 605 033)
Net impact	**(4 585 666 446)**	**(31 949 881)**	-	**(4 617 616 327)**	**(1 859 880 804)**	**(8 632 941 851)**

3.5. PM5: Mechanism for Member States to identify areas to fast-track data centre deployment

Under this measure, on the basis of a national data centre strategy/plan, Member States would need to identify areas to fast-track data centre deployment based on shared EU-level criteria (e.g. on connectivity, energy, water), allowing for the pre-selection of strategic sites where permitting procedures will be streamlined. Fast-tracking measures would apply to projects that have a significant social interest. This would be supported by EU level support through a coordination hub, which will provide guidance, model templates and best practices. The toolbox established in the new Regulation on speeding-up environmental assessments would be leveraged for the designated areas, to allow them to benefit from the additional favourable provisions in environmental assessments (overriding public interest, tacit approval, and dispute settlement). Within fast-track areas, maximum timelines for data centre permitting beyond environmental impact assessment should be of 18 months from the date on which a complete application is acknowledged as duly submitted to the point at which construction activities for the new facility begin. This implies that Member States would be required to adopt procedural measures for accelerated data centre deployment.

Impact on data centre deployment acceleration. As above, it is assumed that the data centre growth rate under this option increases to 15%. This uplift reflects the expectation that faster and more predictable processes with lower entry barriers, reduce time-to-market and improve investor certainty, thereby stimulating additional deployment compared to the baseline. A geographic expansion beyond primary and secondary markets is supposed to emerge under this measure, with new regional hubs emerging in Southern Europe, the Baltics, and Central & Eastern Europe. The measure would primarily affect data centre operators, who account for most projects, and cloud service providers (CSPs) that construct and operate their own facilities (around 40% of projects). See Section 2.3.3 for further details. It is assumed that the share of new projects benefitting from this measure increases from 5% in 2027 to 50% by 2036.

Administrative and adjustment costs for data centre operators. If operators choose to build in these areas to benefit from accelerated permitting, they must comply with the technical, environmental and procedural conditions attached to the areas. This gives rise both to administrative costs (i.e. information obligations needed to demonstrate compliance) as well as to adjustment costs (i.e. changes in project design or planning). Even if they are voluntary costs as operators opt into the scheme, they are considered direct compliance costs once participation is decided. Administrative costs arise from the additional effort required to access the area, i.e. preparing a specific application file, familiarising themselves with criteria and national implementing guidance, including connectivity, energy and water benchmarks, completing standardised templates/checklists and submitting evidence of compliance with area conditions. These costs are assessed following the Standard Cost Model, focusing on the time required for operators to complete these tasks to access fast-track areas. This is estimated as an effort of 20 staff days or 4 weeks (sensitivity range 25-15) per application. This is multiplied by the share of the data centre operators applying for the areas across the EU, since such costs are only incurred by operators that apply to use fast-track areas. This is assumed to be 50% of the companies identified as building data centres in the EU.

$$\textit{One-off administrative costs}_{\textit{year t}} = \Delta T \times \textit{labour cost} \times \textit{No. of applications}$$

Operators are also expected to face one-off adjustment costs if their project design/planning shall be adapted to meet the area requirements, e.g., to comply with environmental conditions applicable within the area. For simplicity, adapting workflows/operations to comply with area-specific requirements and accelerated permitting timelines has been estimated to cost each operator additional 40 staff days (30-60 days) to modify the project[48]. After this initial set-up, recurring costs per project to demonstrate area eligibility are expected not to be incremental with respect to the baseline and are thus not represented.

$$\textit{One-off adjustment costs}_t = \Delta T \times \textit{labour cost} \times s \times \textit{No. new facilities}$$

Total costs (one-off adjustment and one-off administrative) for data centre operators under PM5 are thus estimated at EUR 13.8 m (NPV, 10-years)

Direct economic benefits for data centre operators. This measure aims to provide additional benefits by reducing uncertainty over where investments should be directed. By creating a mechanism for Member States to identify fast-track areas, operators avoid wasted effort on non-viable sites. These changes are expected to reduce the number of iterations required and shorten internal and external time commitments. Once initiated, each new deployment in a designated area requires fewer efforts as eligibility is predefined and baseline data on connectivity, grid, water, land use are available. The areas are also assumed to shorten the

[48] CAPEX investments are not considered as part of the adjustment costs as only projects that already comply, or are willing to comply, with the EED and other relevant requirements under the baseline scenario would be eligible to apply for the fast-track areas. As a result, no additional CAPEX beyond what is already required under existing legislation is expected to arise specifically from participation in the areas.

average development cycle for a new data centre facility by an additional 8 months (sensitivity 6-10), thus leading to a total duration from end of procurement to operation of 18 months, assuming the full effect of the above measure (PM4) is also factored in. The improvement in timeline coming from the implementation of the areas identified for simplification fast-track deployment, has been estimated in 8 months average, due to:

- Coordinated spatial mapping, identifying brownfield sites, industrial areas near power infrastructure, and locations with minimal environmental sensitivity (2 months savings).
- Area-level Environmental Impact Assessment (EIA) completed in advance for entire areas (1 month carried out in parallel to the zoning).
- Standardized building codes, infrastructure requirements, and technical specifications (3 months average for building permit).
- Dedicated infrastructure areas, i.e., pre-planned electrical capacity (12 months for grid connection).

As above, to capture these direct economic benefits, the analysis applies a NPV approach to compare the baseline permitting duration with the accelerated scenario and measure the economic value of bringing construction and commercial operations forward, discounted at the project WACC. The NPV gain is also associated with the reduction in PUE foreseen under this measure, as only the most sustainable data centres would be able to benefit from the fast-tracking. In fact, expected improvements in energy efficiency, modelled as a declining PUE, also contribute to reducing operating costs over time. The NPV increase from EUR 58 million to EUR 74 million reflects the combined impact of accelerated commissioning and improved operational performance, which contribute to the economic benefit of permitting simplification. The business benefit is measured as the difference in net present value (NPV) between an accelerated-permitting scenario and a baseline scenario, discounted at project WACC (6%):

$$\textit{Direct economic benefit}_t = (\Delta NPV = NPV_{PM5} - NPV_{baseline}) \times s \times \textit{No. new facilities}$$

Where each NPV is computed over a 10-year horizon and includes all cash flows: CAPEX outflows during construction, OPEX, Revenues. The analysis has been carried out in nominal terms, with both costs and revenues indexed over time and discounted using a nominal WACC.

NPV baseline (EUR m)	58.32	**Economic benefit per project (EUR m) timeline reduction of 8 months**	
NPV after PM implementation (EUR m)	74.89	16.58	28%

As mentioned above under PM4, a small share of this economic benefit (around 1%) is expected to direct administrative cost savings, i.e. avoided work by staff and consultants (around 1.5 FTE-years) that would otherwise be needed for document preparation, follow-ups with authorities, and procedural back-and-forth foreseen before building a new data centre project.

Under this policy option, the project's internal rate of return would consequently increase by over 80 basis points with respect to the baseline. Taken together, PM4 and PM5 would increase the project's IRR from 9.86% to 10.70%, i.e. an economically meaningful shift which is expected to improve investor appetite. 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. Together, these perspectives illustrate why moving a project from 9.9% to 10.7% IRR can reposition assets within investor target bands, improving competitiveness versus alternative infrastructure investments and affecting bankability. 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.

Total direct economic benefits for data centre operators under PM5 are thus estimated at EUR 11.8 bn (NPV, 10-years)

Adjustment and administrative costs for national public authorities. Member States are required to draft strategies for national data centre deployment, where these do not already exist and, as part of these, designate suitable areas for fast-track data centre permitting. This activity is expected to generate mandatory one-off administrative costs for public authorities. Since at least 7 MS already have a national data centre strategy or an analogous document ready or in the making (see footnote 206), 20 Member States are expected to incur additional administrative costs to draft new strategies. These have been estimated as 3 FTEs (1-5 for sensitivity) per Member State. Moreover, each Member State would need to reprioritise resources to set up processes and align national practices with these new rules. This has been estimated as a one-off adjustment cost equivalent to 6 FTEs (4-8 for sensitivity) per Member State.

Member States are also expected to face ongoing administrative costs to update the strategies and the list of suitable fast-track areas for data centre deployment, estimated respectively as 3 FTEs every 5 years and 4 FTEs every year.

Total one-off adjustment, one-off administrative and recurrent administrative costs for national public authorities under PM5 are thus estimated at EUR 79.9 m (NPV, 10-years).

Administrative cost savings for national public authorities. Recurrent savings for national public authorities should also stem from administrative simplifications given the assumed reduction back and forth interactions between authorities and with economic operators, thanks to the clearer requirements from the areas. As above, given that permitting requires around 80 staff days per project by each authority, process redesign and clearer requirements are expected to reduce this to 20 staff days per new data centre project. The analysis thus foresees that the project facilitator and the fast-track approach might reduce overall administrative staff days per project compared with the baseline.

$$\textit{Administrative cost savings}_{PA} = \Delta T \times \textit{labour cost} \times s \times \textit{No. new projects} \times \textit{No. of MS}$$

Total administrative costs savings for national public authorities under PM5 are thus estimated at EUR 110.8 m (NPV, 10-years).

Adjustment costs for the European Commission. The Commission would face one-off adjustment costs to set up the coordination hub. This has been estimated at 3 FTE during the first year. Moreover, recurrent annual adjustment costs are also estimated for the operation of the coordination hub that supports Member States in identifying and designing fast-track areas. This is estimated at 3 staff days per month each year (0.11 FTE/year) covering Commission staff time.

Total one-off and recurrent adjustment costs for the European Commission under PM5 are thus estimated at EUR 0.4 m (NPV, 10-years)

Indirect savings: Similarly to the measure on administrative simplification, this measure has the potential to realise a broad range of indirect positive impacts on the investments climate, better compliance and transparency of operators during the permitting process, as well as an overall improvement of the decision making process.

Sensitivity analysis: Sensitivity analysis focuses on the potential effectiveness of the measure and the ensuring associated regulatory costs, with parameters modelled to consider a changing level of effort to comply with the data centres areas requirements, both in terms of administrative and adjustment costs, as well as to understand how time savings influencing NPV calculations and adoption rates impact potential direct economic benefits. With respect to benefits, the reduction in months saved is varied between 6 and 10 (central 8 months saving) as well as the share of facilities using the areas by 2036, i.e. considering between 30% and 70% (with a central scenario of 50%). Concerning the costs, the additional time considered for administrative and adjustment costs is also varied to reflect the uncertainty about the intensity of the new procedures. The low scenario (min) combines conservative assumptions on effectiveness (6 months saved, 30% uptake by 2036) with higher costs, while the high scenario (max) does the opposite. Sensitivities were also considered for national public authorities, to reflect the uncertainty related to the complexity of setting up the strategies and administering the new processes, considering respectively minimum 1 and 4 and maximum 5 and 8 FTEs.

Results: The aggregated costs and benefits for all stakeholders over the time horizon are summarised in the table below. Operators incur limited administrative and adjustment costs, while they benefit from substantial NPV gains through shorter times to market and reduced uncertainty, and public authorities face moderate administrative costs. The scenarios are largely driven by the NPV calculation which is affected by the number of months and PUE savings that are expected to stem from this new process. This would be expected for simplification measures, whereby the benefits associated with earlier commissioning and reduced delays are economically significant while the costs are limited to a small number of administrative and compliance activities. As participation to use the areas is voluntary, no major regulatory burdens are imposed.

Table 25. Establishing mechanism for Member States to identify areas to fast-track data centre deployment (PM5)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	1 476 159	3 681 647	-	5 157 806	2 057 555	8 903 876
recurrent administrative	-	66 321 846	-	66 321 846	46 367 793	86 275 900
one-off adjustment	12 364 761	9 940 446	245 443	22 550 649	12 436 549	39 465 368
recurrent adjustment	-	-	117 627	117 627	117 627	117 627
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	13 840 920	79 943 939	363 070	94 147 928	60 979 524	134 762 770
Total benefits	(11 844 675 172)	(110 843 709)	-	(11 955 518 881)	(6 219 100 693)	(19 009 669 476)
Net impact	**(11 830 834 252)**	**(30 899 770)**	**363 070**	(11 861 370 953)	(6 158 121 169)	(18 874 906 705)

3.6. PM6: National funding support for data centres

The introduction of public support measures that target clearly defined market failures in line with applicable State aid rules, to support data centre deployment would generate cost and benefits mainly for operators and national authorities. Under this measure, Member States may grant public support to particularly sustainable and strategic data centres deployed within pre-identified areas (see PM5), according to commonly defined criteria.

Impact on data centre deployment acceleration. The baseline capacity growth presents a 12% CAGR in data centre capacity (2025-2036). Under this option, it is assumed that the capacity growth rate increases to 15%. This uplift reflects the assumption that support measures - together with the other PM described above implemented as part of this option – would reduce barriers to investment, accelerate time to market, and improve certainty for operators, thereby stimulating additional capacity deployment. The scope of this measure covers data centre operators and CSPs active in new data centre builds in the EU, while impacts scale with the share of new projects receiving funding. Please see Section 2.3.3 for further details.

Administrative costs for Data Centre Operators. For operators, the one-off administrative costs of participating in such public support measures are modest. Preparing applications, providing supporting documentation and fulfilling reporting obligations are estimated at 0.2 FTE, or 45 days, during the first year. These are estimated as the staff time spent on the application and, where required, verification processes multiplied by the relevant labour costs.

$$\textit{One-off administrative costs}_{\textit{year } t} = \Delta T \times \textit{labour cost} \times \textit{No. of applications}$$

Operators may face incremental costs to meet eligibility requirements. For example, the inclusion of battery storage, waste-heat reuse, or other technologies to improve grid stability and sustainability could raise investment costs. However, these would depend on the nature of the support measure and thus cannot be reasonably quantified.

Total one-off administrative costs for data centre operators under PM6 are thus estimated at EUR 0.7 m (NPV, 10-years).

Benefits for data centre operators. Operators would benefit from direct financial support, for example through tax advantages or incentives, which is expected to reduce their capital expenditure and accelerate or make possible the implementation of data centre projects. These subsidy amounts would represent direct benefits for operators and corresponding costs for public authorities. Nevertheless, given the voluntary nature of the funding scheme (as the Member State must first decide that it wants to implement such a scheme) they have not been quantified as fiscal transfers.

Adjustment costs for national public authorities. For national authorities, in addition to the overall fiscal transfer costs, the set-up and management of the scheme generates new adjustment costs. These are quantified based on the expected effort required by each Member State, assuming that for the design and legal establishment of the scheme during the first year, 4 FTEs (3-5 for sensitivity ranges) are required and entail one-off adjustment costs. These costs are scaled by the number of Member States expected to operate the scheme under low, central and high uptake scenarios (25%, 50% and 75% of MS). Thereafter, processing, evaluation of applications, and monitoring is estimated at 3 FTEs (2-4 for sensitivity ranges) every two years as recurrent adjustment costs for the duration of the grant (assumed to be of 7-years)**.**

$$\textit{Total adjustment costs} = (\textit{one-off adjustment costs} + \textit{recurrent adjustment costs}) \times s \times MS = [(\Delta T \times \textit{labour cost})_{\textit{year } 1} + (\Delta T \times \textit{labour cost})_{\textit{year } 1,3,5,7}] \times s \times MS$$

Total one-off and recurrent adjustment costs for national public authorities under PM6 are thus estimated at EUR 10.1 m (NPV, 10-years)

Cost savings for national public authorities. Administrative savings may be realised where harmonised EU criteria and templates reduce duplication of effort, e.g. estimated at around 1 FTE annually compared with purely national schemes. However, they are deemed negligeable and are not included in the calculations.

Costs for the European Commission. At EU level, modest administrative costs would arise for the oversight and monitoring of Member State schemes. These costs are not accounted for in the calculations.

Indirect benefits: Subsidies for particularly sustainable and strategic data centres may generate public sector benefits through higher tax revenues with positive spillover effects on the advancement of digital objectives. Tax reductions for data centres can also indirectly generate benefits, e.g. in terms of increased capital inflows and improved digital capacity that supports broader economic competitiveness. Such measures would need to be carefully designed to account for their opportunity costs and ensure that the expected benefits justify the reduced fiscal intake. The support measures should also aim to foster energy-efficient, environmentally responsible data centre facilities, contributing to improve digital resilience and service quality for citizens and businesses. These elements have not been quantified in this section.

Sensitivity analysis: Sensitivity analysis was considered for the total administrative costs for the number of public authorities administering the scheme and the effort required to set-it up and manage it in terms of FTEs.

Results: The table below presents the aggregated costs for all stakeholders for the implementation of this measure. Total costs are estimated at EUR 10.8 m. The minimum and maximum ranges are driven by variations in the number of MS wishing to operate the scheme by and the magnitude of staff days involved. Fiscal transfers have no net effect when aggregated across stakeholders, i.e. financial benefits for operators are mirrored by equivalent fiscal costs for public authorities. Indirect opportunity costs for operators participating in the scheme are also illustrated in the table below and vary based on the uncertainty with respect to the number of applications and days dedicated to proposal/application preparation.

Table 26. National funding support measures for data centres (PM6)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	654 225	-	-	654 225	169 614	1 332 680
recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	3 313 482	-	3 313 482	1 242 556	6 212 779
recurrent adjustment	-	6 830 638	-	6 830 638	2 276 879	13 661 275
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	645 225	10 144 120	-	10 798 344	3 689 049	21 206 734
Total benefits	-	-	-	-	-	-
Net impact	**645 225**	**10 144 120**	**-**	**10 798 344**	**3 689 049**	**21 206 734**

3.7. PM7: Set deployment targets and monitor progress

The measure sets EU-level deployment targets for data centre capacity (e.g., MW IT load) which should be regularly adjusted in light of a monitoring of the compute-capacity gap identified for the EU. Such monitoring would be carried by the Commission and verified by relevant national authorities. The measure does not create mandatory obligations for private operators. The main costs would fall on the Commission, which would be responsible for developing the methodology and compiling the initial dataset. In so far as possible, the methodology would build on existing publicly available data and the data collected as part of the energy efficiency monitoring of the Energy Efficiency directive, and operators are expected to incur limited costs associated with providing supplementary information, while national authorities would face small recurrent costs to verify and validate the data submitted.

Impact on data centre deployment acceleration. As above, under this option, it is assumed that the capacity growth rate increases to 15%.

Administrative costs for Data Centre Operators. Operators are expected to face minor recurrent administrative costs to provide supplementary information need for the dataset. These tasks involve supplying data that they already hold for operational or reporting purposes, notably covering capacity in MW or FLOP[49], which would keep the burden at a minimum. These costs have been modelled as staff time spent participating in surveys and possibly validating data quality. This is expected to require approximately 1 day per year (0.5-1.5 for sensitivity ranges). Annual updates are assumed to entail the same cost.

$$\textit{Total recurrent administrative costs (voluntary)} = (\Delta T \times \textit{labour cost} \times \textit{No. of operators})$$

Total administrative costs for data centre operators under PM7 are thus estimated at EUR 0.4 m (NPV, 10-years).

Costs for national public authorities. National authorities would incur limited recurrent enforcement costs. Their main effort would entail performing periodic checks to verify that the compiled data is complete and reflects national conditions. In this context, the monitoring effort should take into consideration the implementation of national data centre strategies and track progress against their objectives so that any relevant results are also shared with the Commission. This effort is expected to require approximately 15 staff days per year (10-20 for sensitivity ranges), resulting in small and predictable administrative burden.

$$\textit{Total recurrent enforcement costs} = \Delta T \times \textit{labour cost} \times \textit{No. of MS}$$

Total enforcement costs for national public authorities under PM7 are thus estimated at EUR 0.9 m (NPV, 10-years).

Costs for the European Commission. The Commission would be responsible for carrying the study and publishing the results at EU level. This would result in one-off adjustment costs to set up the process and guidance effort, estimated at 1.5 FTEs (1-2 for sensitivity ranges) in year 1, including the procurement of a study to survey capacity periodically over 10-years, with an estimated budget of EUR 800 000. Recurring enforcement costs for monitoring and coordinating with Member States' have then been estimated for at 25 days per year or 0.1 FTEs.

[49] Floating point Operations Per Second (FLOPS) is a standard measure of the performance of a computer, indicating how many calculations on numbers with decimal points it can perform in one second.

Total one-off adjustment and recurrent enforcement costs for the European Commission under PM7 are thus estimated at EUR 1.0 m (NPV, 10-years).

Indirect impacts. The measure generates relevant indirect benefits. For operators, clearer EU-wide targets are expected to reduce investment uncertainty and effort in oversupplied locations. It is expected to create better conditions for operators to understand regional demand and supply gaps and get access to EU-wide benchmarking on capacity utilisation and build-out. In addition, one harmonised EU reporting would reduce duplication of data reporting at national level. National authorities would benefit from improved infrastructure foresight and visibility of national data centre capacity, with better planning for grid reinforcements and targeting of support schemes. The Commission would ultimately also benefit through reduced duplication of studies, easier cross-DG coordination, and enhanced credibility when engaging with international partners. It would benefit from a cross-border, EU-wide analysis of capacity availability and needs to improve evidence-based policy intervention. Wider economic benefits include improved sector planning, enhanced competitiveness and potentially better environmental outcomes.

Sensitivity analysis: Sensitivity analysis has been performed to understand the possible direction of costs, i.e. FTE resources needed by operators, authorities and the Commission to participate in this monitoring exercise. Min and max scenarios vary the central assumptions presented above by approximately ±33%, resulting in conservative, central and optimistic estimates of total costs.

Results: For this measure, total estimated costs for the implementation are modest at EUR 2 266 361. These costs reflect the recurrent adjustment and recurrent administrative costs mainly borne by the Commission staff and national authorities for monitoring activities.

Table 27. Set deployment targets and monitor progress (PM7)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	392 445	-	-	392 445	196 222	588 667
one-off adjustment	-	-	899 421	899 421	858 513	940 328
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	902 108	72 388	974 496	659 316	1 289 676
Total costs	392 445	902 108	971 809	2 266 361	1 714 051	2 818 671
Total benefits	-	-	-	-	-	-
Net impact	**392 445**	**902 108**	**971 809**	**2 266 361**	**1 714 051**	**2 818 671**

3.8. PM8: EU Funding for R&D and innovation ecosystems for cloud and AI

Under this measure, the Commission would identify key R&D funding challenges for the development of energy and resource efficient and secure data centre technologies, including advanced cooling, renewable energy and storage integration and AI-based optimisation tools. Funding schemes would be used accordingly to develop R&D and innovation ecosystems focused on cloud and AI data centres and innovative software enabling cloud and AI computing services across the European cloud-to-edge continuum. The measure would aim to de-risk and accelerate the uptake of advanced, sustainable and secure technologies, with a focus on data centre technologies to improve the replicability and scalability of innovative solutions across

Member States, especially for smaller providers. The measure assumes that successors to today's Horizon Europe exists in the next multiannual financial framework and is provided for modelling purposes only, with no pre-emption of future budgetary decisions. The time horizon considered is seven years, with Work Programmes designed every two years. The scope covers activities at technology readiness levels four to eight, ranging from laboratory-scale research through piloting and demonstration, and includes sustainable cooling and energy solutions, reuse of waste heat and AI-enabled operations.

Impact on data centre deployment acceleration. The baseline capacity growth presents a 12% CAGR in data centre capacity (2025-2036). Under this option, it is assumed that the capacity growth rate increases to 13%. The scope of this measure covers CSPs and operators active in new data centre builds in the EU, while impacts scale with the share of new projects receiving funding. See Section 2.3 for further details. It is assumed that the share of new projects benefitting from PO1-C increases from 10% in 2026 to 50% by 2036 (see also sensitivity section).

Administrative costs for data centre operators. Shall they wish to apply for this type of funding businesses would face administrative one-off costs include proposal preparation and consortium coordination. These costs (e.g. for preparing applications, providing supporting documentation and fulfilling reporting obligations) have been estimated at 0.2 FTEs, or 45 days during the first year for consortium building and design of governance structures. It has been assumed that 20 proposals would be prepared every 2 years. These are estimated as the staff time spent on the application multiplied by the relevant labour costs.

$$\text{One- off administrative costs}_{\text{year } t} = \Delta T \times \text{labour cost} \times \text{No. of applications/proposals}$$

Total one-off administrative costs for data centre operators under PM8 are thus estimated at EUR 1.1 m (NPV, 10-years).

Operators may also face incremental costs to meet eligibility requirements.

Benefits for Data Centre Operators. Operators would benefit from direct financial support, which is expected to reduce their return on investments for cloud and AI projects. These subsidy amounts are considered benefits for operators and corresponding costs for the Commission for transparency, but they do not contribute to the direct impact assessment as they constitute fiscal transfers. Savings are calculated as the amount of reimbursable financing provided to the eligible final recipients. Currently, Horizon Europe Research and Innovation Action (RIA) applies a 100% funding rate while the Digital Europe Programme funding rate is 50% for simple action grants and 75% for the SME Support Actions.

Adjustment costs for the European Commission. The Commission bears responsibility for the management of calls, development of templates and reporting tools, and the evaluation and synthesis of projects**.** The main cost would be one-off programme design and administration, i.e. work programme preparation, call management, evaluation, grant management preparation, monitoring and results dissemination. This has been estimated as 3 FTEs during the first year of the programme and recurring every two years for Work Programme design. Recurrent costs then arise in relation to managing the funding scheme and have been estimated as 1 FTEs. The assumed portfolio consists of one call every two years funding approximately 10 projects.

$$\text{Total adjustment costs} = (\text{one-off adjustment costs} + \text{recurrent adjustment costs}) = [(\Delta T \times \text{labour cost})_{\text{year } 1,3,5} + (\Delta T \times \text{labour cost})_{\text{year } 2,4,6,7}]$$

Total adjustment costs for the European Commission under PM8 are thus estimated at EUR 1.1 m (NPV, 10-years).

There could be an impact for those MS that decide to contribute to the funding programme with national funds in line with applicable State aid rules. As this would depend on the size of this contribution, it has not been modelled under this policy measure.

Indirect savings: the main indirect impact, which is hard to quantify, is the value generated in terms of making current product and services more efficient and competitive and of generating new products and services. The EC estimated that every Euro invested in Horizon Europe generates 11 EUR in economic value (GDP gains by 2045), *i.e. "For every euro of costs to EU society, the programme is expected to generate up to six euros in benefits for EU citizens by 2045. In terms of economic growth, every euro of EU contribution is estimated to generate up to €11 in GDP gains by 2045, according to an evaluation of the Commission released today...*" (April 2025)[50]. The impact of Horizon Europe is directly reflected in the success of funding various research and innovation projects, in January 2025 for example, more than 15,000 projects in fields such as electric vehicles, new antibiotics, and accessible AI technologies benefitted from the programme[51]. A last element has also made Horizon Europe particularly beneficial to European innovation and research savings, with lump sum grants being estimated to reduce beneficiaries' administrative costs from 14% up to 30% over projects' lifetime[52] with the elimination of financial reporting requirements being of paramount importance in stimulating industry participation of SMEs and newcomers.

Sensitivity analysis: Sensitivity analysis was considered for the total costs for the Commission in administering the scheme, i.e. the effort required to set-it up and manage it in terms of FTEs, also to consider the uncertainty related to the overall magnitude of the scheme.

Results: The table below presents the aggregated costs for all stakeholders for the implementation of this measure. Total adjustment costs for the European Commission are estimated at EUR 1.09 m. The minimum and maximum ranges are driven by variations in the effort levels required to operate the scheme by and the magnitude of staff days involved. Fiscal transfers have no net effect when aggregated across stakeholders, i.e. financial benefits for operators are mirrored by equivalent fiscal costs for the Commission. Administrative costs for operators participating in the scheme are also illustrated in the table below and vary based on the uncertainty with respect to the number of applications and days dedicated to the preparation of the proposal/application.

Table 28. EU Funding for R&D and innovation ecosystems for cloud and AI (PM8)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	1 090 375	-	-	1 090 375	678 455	1 599 216
recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	-	694 870	694 870	463 247	926 493
recurrent adjustment	-	-	440 093	440 093	293 395	586 790
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-

[50] See: IP_25_1115_EN.pdf
[51] ibid.
[52] ibid.

recurrent enforcement	-	-	-	-	-	-
Total costs	1 090 375	-	1 134 963	2 225 337	1 435 097	3 112 500
Total benefits	-	-	-	-	-	-
Net impact	**1 090 375**	-	**1 134 963**	**2 225 337**	**1 435 097**	**3 112 500**

3.9. PM9: EU deployment funding for strategic projects

Under this policy measure, without prejudice to the outcome of the negotiations on the next MFF proposal, the Commission would provide financial incentives specifically for data centre projects of European strategic interest and importance according to EU-level eligibility criteria. The measure assumes is provided for modelling purposes only, with no pre-emption of future budgetary decisions. Under this policy option, the EU would act as a market-enabler through financial incentives that de-risk infrastructure investment. By absorbing early capital expenditures (CAPEX) risk in data centre deployment, these investments would incentivise private investments where private return of investment is uncertain. This measure is designed to accelerate the roll-out of secure, sustainable, and cross-border digital services across the Union, while reinforcing European strategic autonomy.

Impact on data centre deployment acceleration. The baseline capacity growth presents a 11% CAGR in data centre capacity (2025-2036). Under this option, it is assumed that the capacity growth rate increases to 14% over the same period. This uplift reflects the assumption that public funding lowers barriers to investment, reduces financing costs for enterprises and accelerates the timing of large-scale deployment projects. Over time, CSPs and operators build more facilities than in the baseline and benefit from public support on a rising share of those builds. The scope of this measure covers CSPs and operators active in new data centre builds in the EU, while impacts scale with the share of new projects receiving funding.

Administrative costs for Data Centre Operators. Even though participating in the funding scheme would be voluntary, it would create administrative costs through financing obligations and administrative compliance requirements. This would include proposal preparation and consortium coordination. Operators would need to prepare proposals and adapt processes to meet eligibility requirements. These would translate into one-off administrative costs incurred every two years in line with the funding cycle. It has been assumed that operators would prepare around 15 proposals per cycle, each requiring staff days (approximately 45 days) of work on average[53]. The average size of consortia has been considered of 2-4 partners per project.

$$\textit{One-off administrative costs}_{\textit{year } t} = \Delta T \times \textit{labour cost} \times \textit{No. of applications/proposals}$$

Total administrative costs for data centre operators under PM9 are thus estimated at EUR 0.8 m (NPV, 10-years).

Operators may also face incremental costs to meet eligibility requirements.

Benefits for Data Centre Operators. As described above, operators would benefit from direct financial support, which is expected to reduce their return on investments for data centre projects. These subsidy amounts are acknowledged as direct benefits for operators and corresponding costs for the Commission, but they do not contribute to the direct impact assessment as they constitute fiscal transfers.

[53] In this report, based on a survey, it was estimated that lump sum proposals required 50 days effort from ideation to submission in H2020 (https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/other/comm/ls-assessment-report-2024_en.pdf).

Adjustment costs for the European Commission. The Commission bears responsibility for the management of calls, development of templates and reporting tools, and the evaluation of projects**.** The main adjustment cost would be one-off programme design and administration, i.e. work programme preparation, call management, evaluation, grant management preparation, monitoring and results dissemination. Aligned with the estimations above, this has been estimated as 3 FTEs during the first year of the programme and recurring every two years for Work Programme design. Recurrent costs then arise in relation to managing the funding scheme and have been estimated as 1 FTEs. The assumed portfolio consists of one call every two years funding approximately 5 projects.

$$\textit{Total adjustment costs} = (\textit{one-off adjustment costs} + \textit{recurrent adjustment costs}) = [(\Delta T \times \textit{labour cost})_{year\ 1,3,5} + (\Delta T \times \textit{labour cost})_{year\ 2,4,6,7}]$$

Total adjustment costs for the European Commission under PM9 are thus estimated at EUR 1.1 m (NPV, 10-years).

There could be an impact for those MS that decide to contribute to the funding programme with national funds in line with applicable State aid rules. As this would depend on the size of this contribution, it has not been modelled under this policy measure.

Indirect savings: the main indirect impact stems from the value generated in terms of making current product and services more competitive and from generating new products and services.

Sensitivity analysis: Sensitivity analysis was considered for the total administrative costs for the Commission in administering the scheme, i.e. the effort required to set-it up and manage it in terms of FTEs, also to consider the uncertainty related to the overall magnitude of the scheme.

Results: The table below presents the aggregated costs for all stakeholders for the implementation of this measure. Total adjustment costs for the European Commission are estimated at EUR 1.1 m. The minimum and maximum ranges are driven by variations in the effort levels required to operate the scheme by and the magnitude of staff days involved. Fiscal transfers have no net effect when aggregated across stakeholders, i.e. financial benefits for operators are mirrored by equivalent fiscal costs for the Commission. Administrative costs (EUR 0.79 m) for operators participating in the scheme are also illustrated in the table below and vary based on the uncertainty with respect to the number of applications and days dedicated to proposal/application preparation.

Table 29. EU deployment funding for strategic projects (PM9)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	792 583	-	-	792 583	446 840	1 235 249
recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	-	694 870	694 870	463 247	926 493
recurrent adjustment	-	-	440 093	440 093	293 395	586 790
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	792 583	-	1 134 963	1 927 546	1 203 482	2 748 533
Total benefits	-	-	-	-	-	-

Net impact	**792 583**	**-**	**1 134 963**	**1 927 546**	**1 203 482**	**2 748 533**

3.10. PM10: EU-level identification of areas for fast-track data centre deployment

Under this measure, the Commission would directly designate areas to fast-track permitting for data centre deployment based on EU-level criteria (e.g. on connectivity, energy, water) and in consultation with Member States experts, allowing for the pre-selection of strategic sites where permitting procedures will be streamlined. Consultation with a newly created EU Data Centre Acceleration Board consisting of Member State experts would be required for the identification and greenlighting of such areas. Permit granting for data centre 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.

Impact on Datacentre data centre deployment acceleration. Under this option, it is assumed that the capacity growth rate increases to 14%. This uplift reflects the expectation that faster and more predictable processes with lower entry barriers, reduce time-to-market and improve investor certainty, thereby stimulating additional deployment compared to the baseline trend. It is assumed that the share of new projects benefitting from this policy measure increases from 5% in 2027 to 50% by 2036.

Administrative and adjustment costs for data centre operators. As above, if operators choose to build in these areas to benefit from accelerated permitting, they must comply with the attached conditions, which give rise to both administrative and adjustment costs. Costs are assessed following the Standard Cost Model, focusing on the information obligations and activities required for operators to access fast-track areas. Reading EU-level guidance, adapting internal procedures and staff would entail one-off costs for each operator. To access areas, operators must familiarise themselves with EU-level criteria. As above, this is estimated as an effort of additional 20 days (sensitivity range 25-15) per operator, which is multiplied by the share of the operators applying for the areas across the EU. This is assumed to be 50% (central value; 30%-70% for sensitivity) of the companies identified as building data centres in the EU.

$$\textit{One-off adjustment costs year } t = \Delta T \times \textit{labour cost} \times \textit{No. of applications}$$

Operators are also expected to face one-off adjustment costs in adapting workflows and templates to comply with area-specific requirements and accelerated permitting timelines. Adapting workflows/operations to comply with requirements has been estimated to cost each operator additional 40 staff days (30-60 days) to modify the project. This would be multiplied by a share of the projects benefitting from the areas across the EU (50% by 2036 as the central scenario; 30%-70% for sensitivity). As outlined above, CAPEX investments are not considered as part of the adjustment costs as only projects that already comply, or are willing to comply, with the EED and other relevant requirements under the baseline scenario would be eligible to apply for the fast-track areas. As a result, no additional CAPEX beyond what is already required under existing legislation is expected to arise specifically from participation in the areas.

$$\textit{One-off adjustment costs} = \Delta T \times \textit{labour cost} \times s \times \textit{No. new facilities}$$

After this initial set-up, recurring costs per project to demonstrate eligibility are expected not to be incremental with respect to the baseline and are thus not represented.

Total costs for data centre operators under PM10 are thus estimated at EUR 11.9 m (NPV, 10-years).

Direct economic benefits for data centre operators. This measure aims to provide additional benefits by reducing uncertainty over where investments can be facilitated, similarly to PM5 but at European scale. With fast-track areas, operators should be able to avoid much of the wasted effort on non-viable sites. These changes are expected to reduce the number of iterations required and shorten internal and external time commitments. These savings are modelled using NPV, reflecting a time saving from end-procurement to deployment of 3 months in total (2-4 months for sensitivity ranges). This is assumed because, while this measure is wider than the measure on the fast-track zoning at MS level, the feedback received during consultations with industry highlighted that a top-level identification would be less effective as it would not be able to account in the same way, of geographical and local specificities.

As above, to capture these direct economic benefits, the analysis applies a NPV approach to compare the baseline with the accelerated scenario and measure the economic value of bringing construction and commercial operations forward, discounted at the project WACC. The strong NPV gain is also very sensitive to the strong reduction in PUE foreseen under this measure, as data centres would also be able to benefit from dedicated R&D to optimised energy efficiency and increase their sustainability. Expected improvements in energy efficiency, modelled as a declining PUE, greatly contribute to reducing operating costs over time. The NPV increase from EUR 58 million to EUR 72 million reflects the combined impact of accelerated commissioning and improved operational and energy performance, which contribute to the economic benefit of permitting simplification. The business benefit is measured as the difference in net present value (NPV) between an accelerated-permitting scenario and a baseline scenario, discounted at project WACC (6%):

$$Economic\ benefit_{t} = (\Delta NPV = NPV_{PM10} - NPV_{baseline}) \times s \times No.\ new\ facilities$$

Where each NPV is computed over a 10-year horizon and includes all cash flows: CAPEX outflows during construction, OPEX, Revenues. The analysis has been carried out in nominal terms, with both costs and revenues indexed over time and discounted using a nominal WACC.

NPV baseline (EUR m)	58.32	**Cost savings per project (EUR m) Timeline reduction of 3 months**	
NPV after PM implementation (EUR m)	72.08	13.76	24%

Total direct economic benefits for data centre operators under PM10 are thus estimated at EUR 8.1 bn (NPV, 10-years).

Adjustment and administrative costs for national public authorities. It is assumed that each Member State would need to set up processes and align national practices with these new rules to provide data to the Commission. This has been estimated as a one-off adjustment cost equivalent to 6 FTEs (4-8 for sensitivity) per Member State as they would need to get familiarised with and onboard the new platform and adopt templates to provide data to the relevant EU entity in charge of identifying suitable areas to fast-track data centre deployment. In addition to this, MS would face one-off administrative costs associated to having to appoint delegates to the management board of the EU Data Centre Acceleration Board.

Once the mechanism is operational, authorities would incur recurrent administrative administrative costs to map and upload data on suitable deployment areas onto the EU platform. For this, 3 FTE annually has been assumed. Recurrent adjustment costs are also expected from national authorities' online participation in the EU Data Centre Acceleration Board. For this, participation is estimated at 3 FTE each year per Member State, covering several meetings annually and additional related work.

Total costs for national public authorities under PM10 are thus estimated at EUR 87.3 m (NPV, 10-years).

Administrative cost savings for national public authorities. By using a central EU-based database, Member States avoid repeated ad hoc clarifications with operators on deployment and siting rules for new data centres, thus reducing information obligations and simplifying tasks. On average, savings are estimated at one-third of time saved in terms of staff days, i.e. estimated as 1 FTE (0.5-2.0 for sensitivity ranges) each year, reducing authorities' net administrative burden. Savings for authorities would also results from a centralised EU-level structure that reduces duplication in national-level coordination meetings.

Total administrative cost savings for national public authorities under PM10 are thus estimated at EUR 12.9 m (NPV, 10-years).

Administrative and adjustment costs for the European Commission. The Commission would face one-off adjustment costs to set up the mechanism and the data centre acceleration board. This has been estimated at 8 FTE during the first year, plus costs for the procurement and development of the supporting digital tool (EUR 2.0 m). Recurrent annual administrative costs are also estimated for the operation of the Board and to map and update the list of suitable fast-track areas for data centre deployment, also estimated at 6 FTEs per year. Adjustment costs in terms of maintenance of the tool (EUR 0.8 m) and a budget for procuring periodic external studies and/or expert meetings (EUR 2 m) are also considered to take place every two years on average.

Total costs for the European Commission under PM10 are thus estimated at EUR 16.1 m (NPV, 10-years).

Sensitivity analysis: The parameters are very sensitive to the number of benefitting operators and the assumed time reductions. As above, sensitivity analysis focuses on the potential effectiveness of the measure and the associated regulatory costs, with parameters modelled to consider a changing level of effort to comply with the areas requirements, both in terms of administrative and adjustment costs, as well as to understand how time savings influencing NPV calculations and adoption rates impact economic benefits. The reduction in months saved varies between 2 and 4 (central 3 months saving) as well as the share of facilities using the areas by 2036, i.e. considering between 30% and 70% (with a central scenario of 50%). Concerning the costs, the additional time considered for administrative and adjustment costs is also varied to reflect the uncertainty about the intensity of the new procedures. The low scenario combines conservative assumptions on effectiveness (4 months saved, 30% uptake by 2036) with higher costs, while the high scenario does the opposite. Sensitivities were also considered for national public authorities, to reflect the uncertainty related the annual effort for participating in the new processes. This has been varied considering between 15 days (high-effort) and 5 days (low-effort) per year and expected administrative cost savings generated by the mechanism, ranging from 0.5 to 1.5 FTEs saved per year at EU level under the low and high scenarios. The measure is highly sensitive to assumptions on PUE improvements, which significantly influence overall OPEX. In the absence of PUE reductions beyond the baseline scenario, the NPV would fall to EUR 59.82 million, i.e. only around 3% of projected cost savings. This highlights the critical role of PM8 and PM9 in driving more sustainable and energy-efficient data-centre operations.

Results: The total costs and benefits for all stakeholders are summarised in the table below. Total costs are estimated between EUR 105.5 m and EUR 131.1 m, including administrative and adjustment costs for establishing and maintaining the EU-level mechanism. Total savings are substantial, ranging from EUR 4.8 bn to EUR 12.2 bn, reflecting the expected efficiency gains from faster permitting, coordinated siting, and reduced duplication across Member States. The high-low scenarios are largely driven by the NPV calculation which is affected by the number of months which is perceived to be saved in this process.

Table 30. EU-level identification of areas for fast-track data centre deployment (PM10)

Cost types	**Data centre operators** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	1 476 159	-	-	1 476 159	830 339	2 767 798
recurrent administrative	-	38 698 697	3 822 094	42 520 790	42 520 790	42 520 790
one-off adjustment	10 375 852	9 940 446	2 596 263	22 912 560	13 728 731	37 475 850
recurrent adjustment	-	38 698 697	9 682 334	48 381 031	48 381 031	48 381 031
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	11 852 011	87 337 840	16 100 690	115 290 541	105 460 892	131 145 470
Total benefits	(8 082 059 633)	(12 899 566)	-	(8 094 959 199)	(4 769 247 820)	(12 245 115 194)
Net impact	**(8 070 207 622)**	**74 438 274**	**16 100 690**	**(7 979 668 658)**	**(4 663 786 928)**	**(12 113 969 724)**

3.11. PM11: Creating EU-level harmonized criteria for sovereign cloud and AI computing services

Policy Measure 11 (<u>PM11</u>) establishes a harmonised Union-level framework for 'sovereign' cloud and AI computing services. AI systems 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.

To be considered '***<u>sovereign level 1</u>***', a service must meet the following cumulative criteria:

(i) the service provider must be **established** in the Union (meaning the EEA); and

(ii) the service must be fully operated from computing infrastructure, personnel and assets **located** in the Union; 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 '***<u>sovereign level 2</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, 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[54]; 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) [55]; 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 subcontractors are from a third country or a third country entity, appropriate measures in place to demonstrate the absence of control; and

(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

[54] 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.

[55] 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.

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 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 '***sovereign level 4'***, 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 and 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 cusomter data, including metadata and telemtry 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 and the software lifecycle. This notably implies that the **relevant code** of the service stack can be audited and that the 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'.

Sovereignty is not only cybersecurity. The criteria above deal solely with sovereignty. Cybersecurity and sovereignty are closely related and are complementary. However, they do not focus on the same aspects nor pursue identical objectives.

In this respect, sovereignty goes beyond the technical protection of services. It primarily addresses who exercises control over the data, and under which legal framework this control is exercised. A cloud service can be technically very secure and still be exposed to non-technical risks stemming from the exposure to third country legislation, because it is subject to foreign laws, or because key operations and decision-making are located outside of the EU. In such cases, the residual risk stems from legal obligations rather than from technical vulnerabilities.

Hence, non-technical risks related to the potential access of third-country authorities to the data cannot be fully addressed through technology or cybersecurity alone. Both need to be understood and looked at as complementary measures, not mutually exclusive and partially overlapping. Technical cybersecurity and non-technical risks address different threat vectors. Properly designed security architectures, such as customer-controlled encryption, strict role segregation or data access minimisation can technically constrain the practical ability of a third-country authority to access the data, regardless of the provider's jurisdiction. In this sense, a technical cybersecurity implementation can serve as a meaningful mitigation strategy of a non-technical risk.

Measures that significantly improve sovereignty (e.g. increasing strategic autonomy and resilience, decreasing dependence) may have a limited incremental effect on classical cybersecurity, while they are still justified for regulatory and trust-building reasons. Conversely, some cybersecurity measures such as stronger encryption mechanisms can be implemented without drastic changes to who controls the infrastructure and data or which legal construct governs access, thus resulting in marginal improvements of sovereignty and operational autonomy.

Even when a service is exceptionally well protected from a cybersecurity standpoint, a legally binding request from third country authorities may still compel the provider to grant access to the data, which constitutes a residual risk if robust internal processes are not in place. This risk exists independently of the technical robustness of the service and the service provider and stems from the provider's legal obligations rather than from technical vulnerabilities. For this reason, the way a service provider constructs its whole architecture becomes crucial and typically follows a "cannot comply" paradigm. Under this approach, compliance with external access requests in rendered technically, operationally or legally impossible (see the OVH case in Canada[56]). This is achieved through well-defined governance and control mechanisms, including strict internal processes governing how employees handle access requests, clear delineated roles and responsibilities regarding data access, as well as more organisational measures such as segregation of duties or control over the cryptographic keys (e.g. ensuring that the encryption keys are not accessible to the provider or are held exclusively by the customer). Although these architectures involve additional upfront and operational costs, the majority in personnel, they demonstrably increase assurance and trust for customers, as they reduce the scope for a compelled access to data through the provider and strengthen compliance with sovereignty requirements. Organizations already have clear roles and responsibilities and segregation of duties defined as part of their policies and procedures addressing technical requirements and hence are not considered in the calculations. Only the additional costs such as the definition of the policies and procedures to protect from the requests of third country legislations with extraterritorial reach and the modification of controls are to be considered in the adjustment costs.

Sovereign architectures incorporating measures to address non-technical risks often require separate environments for jurisdiction, stricter network segmentation and redundant infrastructure, thereby increasing the design, integration and maintenance effort compared to a 'single' cloud deployment, and introducing new misconfiguration risks. Complying with non-technical requirements on top of cybersecurity obligations adds significant legal and administrative efforts as providers must demonstrate extensive evidence of compliance and rely on specialised expertise to do so.

One-off adjustment costs for the EC. In the case of the EC the costs for the definition of the harmonized criteria are not to be accounted for as the definition is set in the Act. However, one off adjustment costs to update the definition are accounted for with 0.5 FTE in 2032.

One-off adjustment costs for national public authorities. In the case of National Public Authorities, one-off adjustment costs relate to the adaptation of their procurement templates based on the harmonized criteria provided by the act. As in the case of the Commission, effort has been estimated for both the initial changes and for the ones needed to be done after the

[56] https://www.heise.de/en/news/Canadian-Court-OVHcloud-from-France-must-hand-over-user-data-11092029.html

revision of the harmonized criteria. In the first case, 3 days have been estimated whereas 1.5 days have been considered for the second activity. These values are per Public Administration publishing public procurement of cloud and AI computing services and deciding to voluntarily use the harmonized criteria for sovereignty. Therefore, the formula for the total one-off adjustment costs must be computed as:

*One-off adjustment costs (National Public Authorities) = time needed to adapt the procurement templates * labour costs * number of procuring authorities using the criteria*

Recurrent savings for national public authorities could result from having a clear harmonized criteria for sovereignty. These are considered negligeable.

***One-off adjustment costs in cloud and AI computing service providers*.** The effort to adhere and align with the criteria for sovereignty only applies when these are linked to an official document specifying the request to comply with the criteria for sovereign services for a specific procedure. Negligeable administrative costs for cloud and AI operators is assumed since voluntary in nature. This has been contrasted with stakeholders as part of the study led by Technopolis group.

***Recurrent savings in cloud and AI computing service providers*.** No recurrent savings are assumed.

Indirect savings: The availability of harmonized criteria would create some certainty on what is considered sovereign, avoiding different interpretations. Through this measure, organisations able to adjust their processes to adhere to the criteria will increase trust from cloud consumers and potentially resulting in larger market revenues for EU providers due to market credibility.

Sensitivity analysis: The data presented above is sensitive notably to the number of procuring authorities under consideration. This has been set between a minimum of 50% and a maximum of 100%. The average value is set to 75% of public authorities. Another important aspect is the estimation of the percentage of procurement procedures that will voluntarily request the alignment with the harmonized criteria for sovereignty.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. The results point towards low total costs for National Public Authorities and negligeable costs for cloud and AI computing service providers. The total estimated costs for the implementation of this measure are EUR 336 077 over the entire period. These costs entirely stem from one-off adjustment costs. The main driver in the min and max values is the number of countries that adopt the EU-level definition for their procurements.

Table 31. Creating an EU-level harmonized criteria for sovereign cloud and AI computing services (PM11)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	336 077	-	336 077	224 051	448 289
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-

Total costs	-	336 077	-	336 077	224 051	448 289
Total benefits	-	-	-	-	-	-
Net impact	-	**336 077**	-	**336 077**	**224 051**	**448 289**

3.12. PM12: Creating EU guidelines for sovereign Cloud AI computing services for public procurement

The assumptions detailed for PM11 remain valid for PM12, with the following additions: Whereas PM11 only considers the criteria of what constitutes a sovereign cloud and AI computing service, PM12 adds detailed guidelines developed by the Commission over PM11's criteria to ensure that service providers interpret them in a similar manner. While the Commission is the sole responsible for the drafting of the guidelines, these would be consulted with representatives of national public authorities and service providers.

One-off adjustment costs for the European Commission stems from the development and adoption of the EU guidelines for sovereign cloud and AI computing services. Guidelines entail detailed explanations and interpretations and therefore the effort estimated to draft and adopt them is 2 FTEs over 1 year.

One-off adjustment costs for national public authorities include the following items: firstly the participation of Member States' authorities in the discussions to draft the guidelines in collaboration with the European Commission and the cloud and AI computing service providers and secondly, the adaptation and updates of the bid templates as well as the institutionalisation of certain elements so that the guidelines can be applied uniformly across the public sector.

The participation in the discussions for the guidelines has been estimated to 27.5 days per public authority considering one participant per MS, while for the adaptation of the templates the estimation is 3 days per public authority applying the guidelines, assuming that 904, the majority of public administrations of the procuring authorities adopt them. A sensitivity is introduced as a minimum of 3 days and a maximum of 10 days.

*One-off adjustment costs (NPA) = labour costs * ((effort in discussions * number of authorities involved in the discussion) + (effort to adapt the guidelines * number of authorities adopting the guidelines)*

Recurrent savings in national public **authorities** may stem from a voluntary but systematic application of the adapted templates in the different procurement procedures. The clarity of the criteria could result in a lower number of disputes between procuring public authorities and cloud and AI computing service providers. However, interviews with Public Administrations do not point to savings as a result of guidelines alone. As part of the sensitivity a min of zero and a max of 5 days per procured tender is arbitrarily set.

*Recurrent savings for reusing the harmonized criteria (national public authorities) = estimated effort saved per tender * labour cost * number of yearly public tenders integrating the guidelines*

One-off adjustment costs for cloud and AI computing service providers. Under this PM, cloud and AI computing service providers will participate in the discussions for the guidelines and the effort estimated for this activity is 20 staff days for 30 cloud and AI computing service providers.

The second type of one-off administrative costs is related to the alignment to the sovereignty guidelines. This requires checking the undertakings' internal organisational and legal procedures. This effort has been estimated in 20 days, and it would apply to all economic operators.

Recurrent adjustments costs in cloud and AI computing service providers. Under this measure no adjustments costs for companies to comply with the requirements and modify organisational or legal procedures, set by the guidelines.

Recurrent savings in cloud and AI computing services providers result from the systematic application and reuse of the documentation that needs to be handed in for each procurement procedure. cloud and AI computing service providers will be able to re-use a set of documents throughout procurements since these will be aligned with the guidelines. These savings are estimated at 1 day per tender and 10 tenders a year.

*Recurrent savings (cloud and AI computing service providers) = effort saved per bid * labour costs * number of yearly bids per provider * number of cloud and AI computing service providers aligned to guidelines*

Indirect savings: Through this measure, organisations able to adequate their processes to adhere to the harmonized criteria for sovereign services will increase trust from cloud consumers and potentially resulting in larger market revenues for EU providers due to market credibility.

Sensitivity analysis: The items used for the sensitivity analysis are 1) the percentage of public administrations using the harmonized criteria for sovereign services in their procurement activities, ranging from 50% to 100%; 2) the number of public administrations procuring cloud services; 3) time needed by public administrations to adopt the procedures as well as to evaluate the bids; 4) the number of cloud and AI computing service providers that can participate in procurement processes, ranging from 244 (min) to 350 (central and max).

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. The average scenario is slightly above cost neutral. While the min scenario measure points towards benefits not fully offsetting costs the max scenario points towards net benefits. The main source of difference between the min and max is caused in the cost savings category and how many national public authorities integrate the guidelines to their tenders and cloud and AI computing service providers adopt the guidelines.

Table 32. Creating EU guidelines for sovereign cloud and AI computing services for public procurement (PM12)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-	-	-	-	-	-
one-off adjustment	2 975 585	1 252 254	168 538	4 396 376	2 562 268	7 021 802
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	2 975 585	1 252 254	168 538	4 396 376	2 562 268	7 021 802
Total benefits	(6 693 922)			(5 693 922)	(1 897 974)	(16 358 845)
Net impact	**(2 718 336)**	**1 252 254**	**168 538**	**(1 297 545)**	**664 294**	**(9 337 043)**

3.13. PM13: Annual conference on digital sovereignty

This policy measure aims at creating awareness and foster discussions on digital sovereignty, sharing latest developments, best practices and solutions among different stakeholders such as policymakers, cloud and AI computing service providers, researchers, or financial institutions. It answers the call made by several cloud and AI computing service providers to gain visibility through political exposure.

The event will be organised on a yearly basis and is expected to last for a week in a venue outside of the European Commission. The target number of attendees is 300 people from the private sector, 3 representatives from each member state national public administration and 100 representatives from the EUIBAs, whose costs are for modelling purposes assigned to those of the Commission.

Recurrent adjustment costs for the European Commission, which result from the organisation and attendance to the conference. EUR 35 000 per day, are estimated for subcontracting costs covering organisation, logistics and operational activities. This includes venue rental, communication with panellists, registration and admission process, badges and catering. For the organisation, it is estimated that 50 staff days will be needed every year by the Commission to oversee the activities carried out by the subcontractor. It is assumed that 5 officials from the Commission will attend all 5 days and require additional 2.5 days for the preparation of their participation in panels, keynotes or discussions. Travel costs are also considered.

Recurrent adjustment costs for national public authorities. 3 representatives per Member State will attend and participate with an estimated effort of five days attending the event and 0.5 to 2.5 days for the preparation of their participation in panels, workshops or discussions. Travel costs of EUR 700 per participant are considered.

Recurrent adjustment costs (NPA) = MS[57] ** Number of participants (PA) * (labour cost * (number of days attending the conference + number of days preparing the workshop) + travel costs per participant)*

Recurrent savings in National Public Authorities. Public authorities will potentially achieve savings staff from a reduction in the effort on bilateral exchanges with other stakeholders. However, given the limited scale of this effect this has not been monetised.

Recurrent adjustment costs for cloud and AI computing service providers (and other stakeholders). An effort between 5.5 and 7.5 days for the participation and preparation of the event are considered for each of the 300 participants from private sector companies and other stakeholders. Additionally, travel costs are included.

*Recurrent adjustment costs (CASP) = Number of cloud and AI computing service providers participating * ((number of days for the preparation and attendance * labour cost) + travel costs)*

Recurrent savings in cloud and AI computing service providers (and other stakeholders). Event participants may save staff days from a reduction in the effort on bilateral exchanges**.** Given the limited scale of this effect this has not been monetised.

Indirect savings:

[57] MS unless stated otherwise is MS = 27

- For cloud and AI computing service providers, faster and better understanding of the technologies and techniques to be secured and sovereign, hence delivering services into the market that are perceived as more trustworthy and more up to date in terms of the use of for instance dependency analysis tooling, ultimately leading to an increase in market sales.
- For national public administrations: a clearer perception of what are the main risks associated with the use of non-sovereign solutions, potentially reducing research on attack and threat vectors, and ultimately resulting in an improved business continuity of the digital services offered.

Sensitivity analysis: The impact of this policy measure depends on the number of events and participants, but a sensitivity analysis is not relevant given the size of the impact.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. Low costs are assumed for all stakeholders modelled. Savings are negligeable and hence not monetised.

Table 33. Annual conference on digital sovereignty (PM13)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-	1 972 376	-	1 972 376	1 972 376	1 972 376
one-off adjustment	-	-	-	-	-	-
recurrent adjustment	12 099 496	-	4 594 816	16 694 311	16 694 311	16 694 311
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	12 099 496	1 972 376	4 594 816	18 666 687	18 666 687	18 666 687
Total benefits	-	-	-	-	-	-
Net impact	**12 099 496**	**1 972 376**	**4 594 816**	**18 666 687**	**18 666 687**	**18 666 687**

3.14. PM14: Interoperability flanking measures

Under this policy measure, the goal is to prioritise the support and development of new harmonised standards under the Data Act in order to cover existing gaps and foster interoperability among cloud services.

This policy measures therefore focuses on three aspects. Firstly, a contract for supporting the Commission in continue analysing the gaps in standardisation, notably in PaaS and SaaS and creating awareness of this lack of harmonised standards. Secondly, on the creation and monitoring of coordination groups steered by the Commission with MS and industrial players for potential recommendations on the prioritisation of standard development. Thirdly, on the development of standards by European Standardisation Organisations (ESO). The conservative approach is that two standards will be developed and adopted yearly.

The application of the standards is out of the scope of the current policy measure.

One-off adjustment costs for the European Commission are related to the budget reserved for the contract on carrying out the studies (EUR 200 000) as well as for drafting the specifications (0.25 FTE). It also includes an external study on portability of AI models, valued at EUR 200000.

*One-off adjustment costs = external study + (effort for drafting the specifications * labour costs) + study on portability of AI models*

One-off administrative costs for the European Commission stem from the setting up of the coordination group, which would hold participants coming from the industry and MS, estimated in 2 FTEs.

*One-off administrative costs = effort to set up the coordination group * labour costs*

Recurrent administrative costs for the European Commission include, firstly, the administrative support for the coordination of standards, both in the coordination group and in the ESOs estimated in 2 FTEs. Secondly, it includes the administration of a support action (2% of administrative overheads), funded under an R&D programme, fostering the participation of European stakeholders in ESOs and standardization activities. The budget estimated for this action is EUR 6 million, within a funding period of 6 years.

*Recurrent administrative costs = labour costs * (effort estimated to monitor the coordination group + effort to monitor the coordination with standardization organizations + effort for the programme administrations)*

One-off administrative costs for national public authorities are the result from MS selecting the members that would participate in the coordination group set up. This is estimated in 0.1 FTE.

*One-off administrative costs (NPAs) = MS * effort to identify members * labour costs*

Recurrent administrative costs in national public authorities stem from the participation in both the coordination groups and standardisation organisations (0.25 FTE for each activity) on a yearly basis. Since ESOs offer the possibility to participate online in the meetings this has been the option considered, and travel costs neglected.

*Recurrent administrative costs (NPAs) = MS * (effort to participate in ESOs + effort to participate in coordination groups) * labour costs*

One-off adjustment costs for cloud and AI computing service providers are also related to the setting up of the coordination group, estimated in 0.1 FTE.

*One-off administrative (CASP) = number of participants * (effort to set up the coordination group * labour cost).*

Recurrent administrative costs for cloud and AI computing service providers are related to the participation of the providers both in the coordination groups and ESOs estimated respectively in 0.25 FTE and 1 FTE respectively. Whereas the meetings for the coordination groups are to be more opportunistic, the meetings on ESOs occur on a regular basis[58].

*Recurrent administrative costs (CASP) = number of participants * ((effort to participate in the coordination groups + effort to participate in the ESOs) * labour cost)*

Recurrent administrative costs for European Standardisation organisations occur by supporting the creation, development and publication of standards, as well as by the

[58] Depending on the ESO the meetings of the Joint Technical Committees or Technical Committees are scheduled on a monthly basis.

coordination with the European Commission and the key stakeholders such as the rapporteurs. This effort is estimated in 1 FTE. This stakeholder category is not accounted for the in the CBA.

Indirect savings: For cloud and AI computing service providers, having clear interoperability standards facilitates EU players the entry into established markets, lowers transaction and integration costs and simplifies the management of a multi-cloud / multi-vendor ecosystem. Finally, it also provides enhanced trust, credibility, transparency and auditability.

Sensitivity analysis: For this policy measure no sensitivity analysis has been considered, given that only the development of standards is considered while the enforcement and compliance by cloud and AI computing service providers are out of scope.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. Low costs are assumed for all stakeholders modelled. Savings are negligeable and hence not monetised. Sensitivity analysis does not apply.

Table 34. Measures to effective interoperability of cloud and AI computing services (PM14)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**SDOs** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	11 205	170 644	-	168 538	350 387	350 387	350 387
recurrent administrative	2 134 177	10 917 230	1 437 660	1 546 004	16 035 070	16 035 070	16 035 070
one-off adjustment	-	-	-	368 538	368 538	368 538	368 538
recurrent adjustment	-	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-	-
Total costs	2 145 381	11 087 874	1 437 660	2 083 079	16 753 994	16 753 994	16 753 994
Total benefits	-	-	-	-	-	-	-
Net impact	**2 145 381**	**11 087 874**	**1 437 660**	**2 083 079**	**16 753 994**	**16 753 994**	**16 753 994**

3.15. PM15: Voluntary sovereign risk assessments for the use of cloud and AI computing services in the public 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 or more frequently 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 NIS 2 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[59] or Italy[60].

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.

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.

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 service providers shall submit the relevant evidence that demonstrate that they comply with the sovereignty assurance criteria to the designated competent authority. For assurance level 1, the service provider will submit the competent authority their self-assessment report for the service. Cloud computing service providers qualifying as SMEs will not be required to undergo the validation by the national competent authority. Verifying the compliance of the service against sovereignty level 2-3-4 would be done through third party's auditors. In this case, the service provider will submit the audit report and the 'positive' audit opinion to the competent authority of the country of establishment who shall verify them, along with the submitted evidence, without undue delay. The result of this activity is an acceptance or rejection of the audit report and opinion.

If a cloud service provider wants to participate in public procurement procedures across the Union, the validating Member State shall notify the other Member States for a review of 60 days.

During the period of review there is a recourse possibility for the Member States. If no reasoned objection has been submitted in the framed period the validation of the audit report and audit opinion shall be considered accepted by all Member States and the service recognized across the Union. If continued objections are raised, the Commission shall adopt a binding opinion.

The competent authorities should register the decision 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.

---

[59] See Cloud in Government Services

[60] See Strategia Cloud Italia

To cater for market evolutions, the sovereignty criteria of all levels and evaluation evidence proposed, but not limited to, would be modifiable by comitology. This evaluation evidence 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 assessment would be peridoically renewable following the same evaluation methodology.

Policy measure 15 then implies that the Commission sets up and maintains a repository of the services audited against level 2-3-4.

Finally, policy measure 15 implies the actual transfer cost for public authorities to change from a non-sovereign service to a sovereign service (cloud porting).

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 PM15 will also contribute to decreasing the overall reliance on non-European cloud and AI computing services, which is SO3.

One-off adjustment costs for the European Commission

Setting up and maintaining the repository of sovereign cloud and AI computing services. These costs include the drafting of the tender specifications for an external provider to build, develop and maintain the repository plus additional time for the evaluation and the definition of their governance procedures. This has been estimated to 120 staff days. The repository will be developed by an external contractor with a contract value of EUR 500 000.

*One-off adjustment costs (EC) = time to draft tender specifications for the repository * labour costs + external contract to develop the repository*

Guidelines for MS to perform the sovereignty risk assessments. In order to support Member States in the implementation of their sovereignty risk assessments, the Commission will publish guidelines. These guidelines would include the process to carry out the risk assessment, the criteria that would allow them to identify the scope, for instance by means of use cases and / or applications, the data classification process, where the market surveillance or information on sovereign services can be found. The estimated effort for the development and publication of these guidelines is 2 FTEs over 1 year.

Recurrent adjustment costs for the European Commission

Maintenance of the repository for audited services. Another important activity is related to the maintenance of the repository of audited services and related activities, including:

- Yearly hosting costs of the repository, estimated to be of EUR 200 000. The repository will be deployed on a sovereign cloud at the Commissions’ premisses and telemetry and FinOps procedures will be put in place to control expenses.

- Yearly maintenance of the repository, performed by an external contractor, includes the upgrades of the software libraries amidst identified vulnerabilities, correction of errors and bugs and additional features. The estimated effort assumed for this is 2 staff days on a weekly basis.
- Oversight of the repository, including the follow-up of the contractors' activities, estimated in 2 staff days per month.

*Recurrent adjustment costs (EC) = costs of the yearly hosting + external contract for the yearly maintenance of the repository + (number of days for the oversight of the repository * labour costs)*

One-off adjustment costs for public authorities.

Conduct the risk assessments. National public authorities and regional or federal authorities in the case of decentralized Member States shall perform at one sovereignty risk assessment, with the aim of mapping sovereignty assurance levels to cloud and AI computing services used in the public sector, taking into consideration aspects such as sensitivity and criticality of the data processed, the risks associated to the potential unlawful access to data by third country legislation, potential disruption of the services, and the existence of computing services audited under that sovereignty level, among others. The estimated number of authorities is 267, considering the NUTS-0 and NUTS-1 distribution. Given that it is a voluntary measure, it is considered that the uptake will be only by in 25% of the authorities, that is, 67.

The output of this risk assessment will be a classification of applications or use cases categories mapped to the minimum sovereignty assurance level permitted for the procurement of cloud and AI services serving those cases.

The estimated effort for this sovereignty risk assessment is of 10 FTEs. This is a new activity for which there is yet few expertise in the Member States. It is considered that in the initial iteration, Member States will need to understand well the sectors, applications and type of data, among other aspects, that will drive their risk analysis to decide one sovereignty assurance level or another. It is expected that initially this will be an activity encompassing various ministries and agencies and therefore an intensive collaboration is expected. The guidelines from the Commission, however, should alleviate this effort.

The risk assessments will start in 2029, once EUCS and the sovereignty framework is in place.

Designation of the competent authority, which has an estimated of 0.2 FTE per MS, which will be responsible to verify the audit reports received from the providers that had their services audited at sovereign level 2 at least.

Cloud-to-sovereign-cloud migration costs for the public sector. Detailed information is provided in Annex 12 on the methodology and calculation of the costs for the migration and porting of cloud applications to sovereign cloud services.

Due to the voluntary nature of the measure and given that transition to a sovereignty service is recommended and not mandatory, only 25% of the *cloudified* and the *cloudifiable* IT systems would be ported or migrated to a sovereign solution.

Both the migration of applications from legacy-to-sovereign cloud or from cloud-to-sovereign cloud will be performed in a linear distributed manner in a time frame spanning 5 years, starting in 2029, once there is a set of services audited as sovereign.

The average cost of porting a single application to a new cloud varies from EUR 30 000 and EUR 600 000 depending on the size of the application, and not much on the type of cloud at origin or destination, as they are mainly based on human effort (400 to 8000 hours of work). See Annex 12 for a explanation of these figures.

These costs have not been quantified in the cost-benefit analysis, although they are described in detail, and illustrated with the real use cases in Section 6.1.2 of the main text.

Recurrent administrative costs for national public authorities

Sovereignty risk assessment. This risk assessment shall be renewed every 4 years. The effort estimated for this reassessment of the sovereignty risks is estimated to be 5 FTEs, a lower effort than implementing the risk assessment from scratch, given that the activity is already ramped up and the Member States would already have a good understanding of their situation. 67 authorities will carry out these assessments and therefore will have to renew them.

Revision of the audit reports by the competent authorities, per service audited at sovereign level 2 at least, estimated at 5 days per service. After verifying the audit report, opinion and evidence and consulting with the other competent authorities, the evaluating competent authority will adopt a decision that would allow a service provider to participate in public procurement activities.

Recurrent savings in National Public Authorities

Running applications on the cloud. Operating applications on the cloud, if performed well, with a continuous FinOps verifying that services are not overprovisioned can lead to significant savings. Literature sources estimate that the total cost of ownership (TCO) savings can amount to 20-50% in the case of legacy-to-cloud migrations[61]. No savings are here accounted for in the operation of applications migrated from cloud-to-sovereign cloud, as the applications would have already been benefitting from the total cost of ownership savings. See Annex 12 for a further qualitative discussion on savings.

Simpler public procurement. Savings in this respect stem from the simplification of voluntarily using procuring audited services, which are part of the repository of sovereign cloud and AI computing services. This shall allow public administrations to save time in the verification of the documentation for the evaluation of the offer. This will result in 2 staff days per bid, and assuming that there are 3.5 potential contractors presenting bids in each tender procedure.

*Recurrent savings = Average number of yearly service bids requiring sovereignty assurance level 2 – 4 * staff costs savings per bid*

Sovereign services. The savings from using sovereign services cannot be quantified due to the intangible nature of sovereignty and resilience.

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

[61] Chatzithanasis & Michalakelis (2018) estimates 24% to 50% The Benefits of Cloud Computing:. Ali Khajeh-Hosseini, David Greenwood, Ian Sommerville

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, one of the largest EU service providers of 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.

Benefit wise, cloudifying legacy on-premises services means new revenues. As to the move from traditional cloud to sovereign cloud, today's few available sovereign services come with a mark-up which is still too uncertain to draw conclusions (see discussion under Problem Driver 4 in 2.3.4). To this additional income, consulted EU service providers see also sovereign services as niche market where they have a demonstrable added value that could spill over to other market segments. The consulted companies unanimously indicated that it is too early to confirm whether, over the span of the next ten years, the incremental cost and benefits would reach the same balance (i.e. margins) as with equivalent non-sovereign services, which is today commonly assumed to be around 30%[62]; to cater for this uncertainty, this assessment assumes that stakeholders' margins vary from 25% to 35%.

One-off adjustment costs for cloud and AI computing service providers

Ultimately, the decision of a provider to audit one or more services is their own business decision. However, in order to have a sense of magnitude of how many providers could decide to do so, extensive desk research conducted as part of the preparatory study (Technopolis et al., 2025) identified that services from 59 non-EU headquartered cloud service providers likely meet Level 1 requirements and would be able to qualify to Level 2 should they decide so. 226 EU headquartered providers could qualify their services as Level 2 and would be able to qualify their services as Level 3/4 should they decide so. If only large companies are considered and SMEs are excluded, the figure goes down to 59 EU headquartered large companies.

The assumptions are as follows: 150 services will be audited from 2029 until 2034, with the assumption of 30 audits the first year, and an annual growth of 38%. This builds over the number of services currently qualified in comparable national qualification and certification schemes[63], and the FedRAMP mechanism. As of September 2025. the FedRAMP repository contains 530 authorised services under level moderate and high.

[62] Amazon Web Services profits squeezed as AI arms race drives spending surge – GeekWire
[63] For this impact assessment ES, IT, and FR have been considered as baseline as their data is public.

Services may be audited under different levels, provided that the criteria mentioned above (see PM11) are met. For the purpose of this impact assessment, it is estimated that the proportion of audited services in the different assurance levels will be mirroring the needs of the public authorities (see below). This would then make that out of the estimated 150 audited cloud services:

- 70% of the services will be Sovereignty Assurance Level 1, making 105 services
- 20% of the services will be Sovereignty Assurance Level 2, resulting 30 services
- 9% of the services will be Sovereignty Assurance Level 3, amounting to 13 services
- 1% of the services will be Sovereignty Assurance Level 4, resulting in 2 service.

The effort needed to get audited under sovereignty assurance level 2-4 is estimated to be 15 FTEs. This includes the definition and implementation of the necessary legal, organisational and technical measures to reach sovereignty assurance level 2 – 4 and the auditing procedure carried by the third party auditor. This effort was validated in the Final Validation workshop held as part of the study led by Technopolis.

*One-off adjustment cost of new audits = (effort to get sovereignty assurance level 2 – 4 audited * labour costs) * number of audited services assurance level 2 – 4*

One-off regulatory fee for cloud and AI computing service providers

*New audits***,** assumed to be EUR 20 000, for the estimated number of audited services at sovereignty assurance level 2– 4.

*One off regulatory fee for new audits (CSAP) = regulatory fee * number of audited services assurance level 2 – 4*

Recurrent regulatory fee for cloud and AI computing service provider

*Renewal of audits***,** assumed to be EUR 14 000.

*Recurrent regulatory fee for new audits (CSAP) = regulatory fee * number of audited services assurance level 2 – 4*

Recurrent administrative costs for cloud and AI computing service providers

Audits: These compliance costs stem from the audits to maintain the audit certificate, where the goal is to verify that the conditions under which it was first obtained remain valid (effort estimated as 3 FTE/year per service). Compared to the effort needed to achieve it initially, the effort dedicated to the intermediate audits has been assumed to be lower than obtaining it initially, in spite of the annual reporting obligations set out above.

*Recurrent administrative compliance cost of renewal of audits = (time to be audited * labour costs) * number of audited services*

Recurrent savings for cloud and AI computing service providers.

Audits. A crucial matter in the analysis of the recurrent savings for cloud and AI computing service providers is the single market effect. Providers will be able to be audited in one MS and operate in all EU27 at once. Additionally, the analysis considers that in the business-as-usual scenario one cloud service provider would seek to obtain the audit in 5 MS in average. Given the costs of compliance, a cloud and AI computing service provider would carefully prioritize in which MS(s) it would seek to obtain the audit, usually taking into consideration aspects such as the market share or other commercial opportunities. With this policy measure, a single audit provided by a MS will enable a provider to present offers including the audited service to public tenders in all 27 MS.

*Saving costs audits valid throughout the EU = Number of MS where the cloud and AI computing service providers would get certified in the absence of an EU approach * cost to get audited * number of audited services*

Public procurement. Another relevant saving stems from the fact of not having to collect and resubmit all the evidence necessary to demonstrate that the criteria are fulfilled for each bid, given that the audited services are listed in the repository and accessible for the contracting authority. The assumption is that undertakings will save 5 staff days / year per service and bid. The number of yearly bids amounts to 50 a year.

*Business costs saved: = Businesses time saved per evidence submission in a tender procedure * number of submitted bids*

Recurrent administrative costs for the private sector (Auditors)

Third party audits. In this PM, as mentioned above, the target number of cloud and AI computing services that will be in possession of the positive audit report is estimated to reach 150 by 2032[64], whereas 30 of these will be audited sovereign level 2-4 during the first year. The assumed CAGR is 38%. The assumption under this policy measures follows a linear progressive uptake of the certification scheme.

The estimated average effort for auditing a service under Sovereignty assurance level 2-4 is 110 days / audit. The same effort is considered for the renewal process..

Indirect savings: Through this measure, cloud and AI computing services able to comply with the sovereignty audit scheme will increase trust from public administrations, and notably for the most critical cases. This will result in more trustworthy, credible and very specialized as well as very advanced offers responding to challenges such as resilience and autonomy.

Sensitivity analysis: The most affected parameters for this Policy Measure are as follows: 1) number of FTEs required to get audited and to maintain the audit (min and max value are 10 and 20 respectively). For the maintenance of the audit this varies between 2 and 5; 2) the number of MS that designate the competent authorities to carry out the sovereignty risk assessments. This varies from 5 MS (min) to 27 (MS), with 16 being the central value: 3) in terms of savings, the common audit process will allow to save audit efforts in some of the markets where the provider operates, considered to be a minimum of 3 MS and a maximum of 10, with a central value of 5.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. For all scenarios including the average, min and max the benefits outweigh costs. What causes the range between the min and the mix is dependent on the number of Member States which take up the scheme.

Table 35. Voluntary sovereign risk assessment for the use of cloud and AI computing services in the public sector (PM15)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)

[64] Assumption taken considering the current valid authorised cloud services in FedRAMP moderate and high, which amounts to 531 as of 26 September 2025.

one-off administrative	-	-	-	-	-	-
recurrent administrative	25 161 510	17 314 082		42 475 592	25 383 464	2 763 406 090
one-off adjustment	51 370 998	39 378 999	693 692	91 443 689	59 940 678	247 443 239
recurrent adjustment	-	-	2 117 274	2 117 274	2 117 274	44 128 193
one-off regulatory fees	773 977	-	-	773 977	773 977	773 977
recurrent regulatory fees	1 047 966	-	-	1 047 966	1 047 966	1 047 966
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	78 354 450	56 693 081	2 810 965	137 858 497	89 263 359	232 817 048
Total benefits	(451 348 550)	(3 280 022)	-	(454 628 572)	(172 234 292)	(566 620 181)
Net impact	**(372 994 099)**	**53 413 060**	**2 810 965**	**(316 770 075)**	**(82 970 933)**	**(333 803 133)**

This policy measure would trigger an acceleration of porting of some applications to sovereign cloud services of assurance levels 2 to 4, requiring an anticipation of expenses of EUR 620 m to 4 bn. These costs are estimated and reported under section 12.4 of Annex 4. Since they represent planned expenditure that would be incurred in the future as part of the regular cloud contract renewal cycles and independent of the present policy measure, they have been scoped outside of the summary cost table so as not to conflate structural renewal costs with the incremental financial impact of the measure itself.

The benefits accruing from the risk reduction, notably an increased autonomy and strengthened operational resilience through the adoption of sovereign cloud and AI computing solutions are intangible and cannot be expressed in quantitative terms. While these benefits cannot be quantified, they are acknowledged as a significant consideration underpinning the policy rationale.

3.16. PM16: Non-mandatory specific award criteria for the procurement of cloud and AI computing services

This policy measure defines non-mandatory award criteria for the procurement of cloud and AI computing services, rewarding their specific characteristics in terms of EU added value.

With a view to enabling an enhanced EU value added of public procurement, this measure establishes a set of voluntary non-price award criteria to be included, voluntarily, by contracting authorities in the procurement of cloud and AI computing services. These criteria will earn additional points to tenderers that demonstrate:

(i) Their contribution to reinforcing the digital technology supply chain in the Union, including the use of software or hardware designed or manufactured in the Union
(ii) 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;

Next, the baseline data used for this policy measure is detailed.

Number of public tenders for cloud and AI computing services. The data is taken from the TED portal[65] where all public tenders open by MSs are recorded. The list of tenders is filtered by the CPV related to IT services, software and computing, i.e. CPV codes under the families of 72000000, 30000000, and 48000000, and by keywords "cloud" and "AI", which results in 1.043 tenders for 2024. This is expected to grow until 2030 using the same CAGR as the one observed for these tenders in the period 2021-24 (8.6%). From 2031 until the end of the period, the CAGR is reduced to half (4.3%) as a result of the improvement in cloud and AI adoption. It is assumed that one fourth of the tenders use the voluntary criteria.

The assumption is that all national public authorities participate in this measure even if not mandatory and each of them receives 3 to 4 offers for each public tender they organise.

Cloud and AI computing service providers that participate in public procurement every year. An estimate of 350 providers is used in the calculation. The estimate is based on a combination of TED and desk research.

One-off administrative costs in national public authorities. Administrations that choose to adhere to these criteria will need to adapt their procurement templates by integrating the specific award criteria, with a low effort of up to 10 staff days for each public authority. This is translated into the corresponding cost by multiplying by the average salary and the number of public authorities introducing the specific award criteria. It is assumed that 25% of the authorities decide to use the award criteria in their tenders and hence make the corresponding changes.

One-off administrative costs (NPA) = number of national public authorities introducing the non-price award criteria
*(labour cost * effort to adapt templates)*

Recurrent savings in national public authorities. Public authorities will use the standard award criteria and guidelines instead of drafting those separately. This represents a saving and is estimated at an assumption of 1.5 days per public tender.

Recurrent savings (NPA) = number of tenders
*(labour cost * effort saved)*

One-off adjustment costs for cloud and AI computing service providers. Providers who choose to participate in procurement processes including the specific award criteria need to align with the public procurement procedures for cloud and AI computing services. This includes adopting and aligning their processes and improving them to meet these criteria, with an estimated one-off effort of up to 20 staff days.

Recurrent administrative costs for cloud and AI computing service providers, are the costs needed to adequate the offers, assumed to be 2 staff days per bid. These days were validated during the interviews as part of the supporting study. They assume only administrative work for companies who would be eligible. The cost is calculated multiplying this effort by the

[65] EU-Tenders search APIs: https://docs.ted.europa.eu/api/latest/search.html

number of bids presented in a year and the average salary of the cloud and AI computing service providers.

*Recurrent administrative cost = number of bids presented * effort / bid * labour costs*

Recurrent savings for cloud and AI computing service providers. Revenue gains are possible, especially for providers who can differentiate due to the award criteria. These are however not modelled.

Indirect savings: There are notable indirect benefits for cloud and AI computing service providers that are able to comply with the different non-specific award criteria. For instance, additional revenue gains, increase in reputation and the possibility to enlarge the scope of their solutions which in turn may lead to an increase of sales.

Sensitivity analysis: The impact of this policy measure is sensitive to the number of public authorities procuring cloud and AI computing services, the number of tenders and offers per year and the number of cloud and AI computing service providers and the costs to adapt the offers.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. Total costs are estimated between EUR 6.0 million and EUR 31.5 million, consisting mainly of recurrent administrative costs related to coordination, reporting, and compliance activities, alongside smaller one-off administrative and adjustment costs. Total cost savings are limited, ranging from EUR 1.1 million to EUR 3.3 million. Costs outweigh benefits across the average, min and max set of parameters. The difference in the min and max is mainly caused by the number of CSP and AI providers participating in public procurement every year across EU.

Table 36. Non-mandatory specific award criteria for cloud and AI computing service procurement (PM16)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	1 731 580	-	1 731 580	865 790	2 597 370
recurrent administrative	13 486 479	-	-	13 486 479	3 371 620	23 601 338
one-off adjustment	3 560 007	-	-	3 560 007	1 780 004	5 340 011
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	17 046 486	1 731 580	-	18 778 066	6 017 413	31 538 719
Total benefits	-	(1 630 135)	-	(1 630 135)	(1 086 757)	(3 260 270)
Net impact	**17 046 486**	**101 445**	-	**17 147 931**	4 930 657	28 278 449

3.17. PM17: Public Sector Cloud Federation

PM17 establishes a European public sector cloud federation for voluntary participation European and national public authorities at all levels to allow them to share their own existing data centre, cloud and AI computing services. This policy measure requires the establishment of the technical back end that operates the necessary brokering services.

Cloud Capacity in the Public Sector. The public sector in Europe is running a data centre capacity of 1.5 GW[66] in 2025 and shows an annual increase of 8.9% due to the growing adoption of PaaS and SaaS services[67], that might be impacted in the first years with this policy measure. As the measure is voluntary, it is assumed that only a part (two thirds) of the public authorities will join the federation, reducing the capacity available in the federation to 1 GW.

Assuming a power usage effectiveness (PUE) of 1.29, a consumption of 500 W per server and 32 virtual machines (VMs) per server, the 1 GW of datacentre capacity could deliver around 50 million mid-sized VMs of 4 vCPU and 16 GB.

$$\text{Number of VMs} = ((1\,000\,000\,000\ W / PUE) / 500\ W \text{ per server}) \times 32 \text{ VMs per server}$$

Market price of a VM is set at 0.23 EUR per hour based on a baseline configuration of 4 vCPUs (processors) and 16 GB (memory)[68]. Considering the high margins in commercial cloud services, beyond 60%, and a cost-based chargeback among participants to the federation, a conservative assumption of a 30% price advantage of the cloud federation services with respect to commercial cloud services is made, setting the cloud federation's VM price at 0.16 EUR per hour. This assumption was confirmed in the Final Validation workshop held as part of the study carried out by Technopolis et al. (2025)).

Over time, VM configurations will evolve to higher performance and higher share of AI processing units (GPUs, TPUs, etc). Prices are considered to remain relatively constant as these more sophisticated configurations will get commoditized over time.

A target utilization of 60% is assumed for the cloud capacity based on own infrastructure. This is based on a report from Berkeley Lab on data centre energy usage[69], considering an evolution of public sector data centres from current low occupation in traditional compute (below 20%), towards higher occupation levels as the load of AI inferencing and AI modelling grows (datacentres with this kind of loads present an average of 40% and 80% time operational, respectively). A middle point (60%) is set as the target.

Applying a conservative approach only 25% of the idle capacity, 10% of the total capacity, is considered to be shared with other members of the cloud federation. On the other hand, cloud capacity extensions in each MS are assumed to be reduced by 10% by using idle capacity from other federation members.

With regards to the number of public authorities that own and run a datacentre infrastructure and could be members of the public sector cloud federation, in the absence of a precise number,

[66] Based on calculations by Technopolis et al. (2025). The study estimates a total computing capacity consumed by the public sector in EU27 in 2025 of 2.9 GW. The CATI surveys shows that 51% of this computing capacity (1.5 GW) is served by datacentre infrastructure own by the public administrations. This is the capacity that is shared in the cloud federation.

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

[68] Example taken from a basic AWS EC2 product using AWS configuration tool: https://calculator.aws/#/createCalculator/ec2-enhancement. Parameters used: <Tenancy:Dedicated Instances>, <Region:Frankfurt>, <Operating system:Linux>, <vCPUs:4>, <Memory:16 GiB>, <Network Performance:Up to 12500 Megabit>. Price calculated at 12th Sep 2025 for <Instance name:m6i.xlarge>: 0,253 USD/hour (0,227 EUR/h at the average exchange rate for 2025 by Sept 2025: 0,8986 EUR/USD)

[69] Shehabi, A., Smith, S.J., Hubbard, A., Newkirk, A., Lei, N., Siddik, M.A.B., Holecek, B., Koomey, J., Masanet, E., Sartor, D. 2024. 2024 United States Data Center Energy Usage Report. Lawrence Berkeley National Laboratory, Berkeley, California. LBNL-2001637. https://escholarship.org/uc/item/32d6m0d1

the assumption made is that there is one in each NUTS1 and NUTS2 area[70], resulting in a figure of 300 public authorities in Europe.

One-off adjustment costs for the European Commission. This policy measure entails one-off adjustment costs to establish the public sector cloud federation platform. These costs include 4 persons half time in 2027 (2 FTE) from the EC to run the procurement process for the federation platform (define requirements and prepare the call, assess and award the contract), that will be tasked to a subcontractor for an estimated cost of EUR 20 000 000. This includes the technical aspects of the platform, as well as the development of the service level agreements and of the technical common specifications.

*One-off adjustment costs = external contract to develop the platform + (effort to run the procurement process * labour costs)*

Recurrent administrative costs for the European Commission. On a yearly basis, the operation of the federation platform requires 6 FTEs.

Recurrent adjustment costs for the European Commission relate to hosting of the platform in a cloud, estimated at 1 million EUR per year, and operating, maintaining and evolving the federation platform, with an effort of 60 contractor FTEs per year, including the integration of APIs and connectors to aggregate the NPA cloud resources to this platform.

Recurrent adjustment costs = hosting of the platform + maintenance of the platform

One-off and recurrent adjustment costs for National Public Administrations. Member States dedicate an effort of 55 staff days (0.25 FTEs) in 2027 to participate in the setup of the public sector cloud federation.

On a recurrent basis during the first years, up to 2031, each NPA will have to apply efforts to connect national infrastructures and ensure interoperability to join the federation (2 FTEs), to onboard cloud resources and services on the federation platform (30 staff days) and to update and delete them later on (20 and 50 staff days respectively), making a total yearly effort of 2.45 FTEs.

Recurrent savings for National Public Administrations. With the measure and thanks to the federation platform, NPAs will save 0.5 FTEs in the coordination with other Member States for the sharing of cloud capacity.

In addition, the sharing of 10% of the idle VM capacity on a pay-per-use mode (with capacity assumed to be consumed during 10% of the time) will represent a charge back of around EUR 690 million EUR inz the first year (2027).

Savings = VM capacity x %shared x price/hour x number of hours

The acquisition of 10% of the cloud capacity demand from the cloud federation will derive in around EUR 296 million EUR savings in 2027, due to the 30% price difference between federation and commercial cloud services.

[70] NUTS1 and NUTS2 areas in Europe are close to 340 (https://ec.europa.eu/eurostat/web/nuts). An adjustment has been made to slightly reduce the number of NUTS2 areas with a public authority owning and running datacentre infrastructure in the bigger markets where the administrative distribution at that level is more granular.

Savings = VM capacity x %extension avoided x price difference x usage

These savings grow over the years with the expected increase in cloud capacity demand (8.9% annually).

Indirect savings: Through this measure, the public sector achieves additional data centre efficiency and improves the return on investment from their infrastructure and assets in cloud and AI. The increase in resource utilization achieved by pooling resources reduces the investment risk and may stimulate the increase in their investment in data centre, cloud and AI capacity.

Sensitivity analysis: The values to be challenged in this policy measure include the capacity shared by each MS with the federation ranging from 5% to 15% which impacts the savings in terms of idle capacity reduction.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. The main difference stem from the percentage of idle resources shared and particularly by the Member States participating in the federation.

Table 37. Public Sector Cloud Federation (PM17)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-	-	4 312 980	4 312 980	4 312 980	4 312 980
one-off adjustment	-	4 613 563	19 540 197	24 153 761	23 231 048	25 076 473
recurrent adjustment	-	213 669 483	99 241 949	312 911 432	269 386 167	356 436 698
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	-	218 283 046	123 095 126	341 378 173	296 930 195	385 826 151
Total benefits	-	(12 533 772 955)	-	(12 533 722 955)	(8 175 327 110)	(16 892 218 800)
Net impact	-	**(12 315 489 908)**	**123 095 126**	**(12 192 394 782)**	**(7 878 396 915)**	**(16 506 392 649)**

3.18. PM18: Vendor-neutral EU cloud/AI skill certificates

The goal of this policy measure is to create a vendor neutral cloud and AI computing services training programme and curricula for the re-skilling and upskilling of workers in key digital technologies for the single market. Targets of these certification and training programmes are individual workers and students, not organisations.

Nowadays, many cloud service providers offer training and certification programmes (see for instance AWS[71], Microsoft Azure[72] or Google[73]) but they are vendor specific and tailored to their technologies. And this, despite the commonalities that exist across different cloud

[71] https://aws.amazon.com/certification/
[72] https://learn.microsoft.com/en-us/credentials/browse/?credential_types=certification&products=azure
[73] https://grow.google/intl/europe/courses-and-tools/?category=career&topic=cloud-computing

platforms: architectural patterns, cloud security controls, and development lifecycle management methodologies, among others.

There are few vendor-neutral cloud skills certification programmes in the market, and they are majorly focused on security[74], leaving aside important aspects such as the design and architecture of cloud native applications, AI services, DevOps, AIOps or FinOps[75]. University degrees include some of these subjects, but they are typically integrated in long studies, target undergraduate students and are not usually available as vocational training for professionals.

Under this policy measure, it will be created a curriculum of vendor neutral courses, as well as their content, both for the materials and the exams. In principle, obtaining these certificates will be a voluntary mechanism intended for developers whereas companies may require them in certain job offers at their discretion.

One-off adjustment costs for the European Commission. The adjustment costs modelled result from the subcontracting of a study under a public tender procedure that will

1) define the gaps on the current skills panorama to develop and deploy cloud and AI computing services prioritising the most relevant areas; and

2) develop the materials and content covering the prioritized areas, including also the exams. Substance-wise, as hinted previously, the main focus is to ensure that existing cloud professionals upskill themselves, from knowing how to use the products from a single vendor to a vendor-agnostic / multi-vendor skill set.

This contract has been estimated at EUR 750 000 and running for two years (2027-2028) with the aim of developing 15 courses. For the drafting of the specifications as well as for the follow up of the implementation of this study, it has been estimated 1 FTE of the Commission. An additional cost at EUR 252 806 was estimated to establish a training accreditation mechanism.

*One-off adjustment costs = external contract + (effort to draft the specifications * labour cost)*

One-off administrative costs for the European Commission. Here the costs to set up the mechanism to ensure the quality of the training materials and the skills certifications are ensured as well as the infrastructure for the training. This is estimated at 3 FTEs spanning for a year.

Recurrent administrative costs for the European Commission stem from the operational costs of running the training certification programme. This is estimated at 1 FTE.

Recurrent savings for the European Commission are the result of having a coordination mechanism that may avoid duplication in the creation of a skills framework or training materials. This has been estimated at 0.25 FTEs.

[74] The most certificates recognized in the market include ISC2 CCSP (https://www.isc2.org/certifications/ccsp) and CompTIA Cloud+ (https://www.comptia.org/en-us/certifications/cloud/)

[75] DevOps is a philosophy that aims to close the gap between the development and operation teams involved in the development and deployment of software applications, including cloud native and focusing on automating the procedures such as integration and deployment. AIOps is a similar concept focusing on the development and operation of AI applications automating also the data pipelines. Finally, FinOps is the means in which financial and development teams can jointly manage the expenditure resulting from deploying services onto the cloud. The goal is to minimize the expense but maximize performance, quality and velocity.

***Recurrent administrative costs for cloud and AI experts*: Training fees are assumed at EUR 100 per training.

Recurrent savings for cloud and AI computing service providers stem from the vendor-neutrality of the proposed certificates. A person aiming to become cloud developer or a cloud architect can obtain one vendor-neutral certification, containing the main principles and patterns that can be applied to every technology with little effort in customisation or learning the specificities of said technologies, instead of getting the certificates from all technologies used. The aim is to avoid the multiplication of costs that currently developers incur by needing to get certified in multiple technologies for their professional development (savings of 3 days per course).

The vendor – neutral certification "Certified Cloud Security Professional CCSP"[76], manages to certify 3,000 – 3,500 people globally per year. AWS reports to have 1.05 million unique individuals certified[77]. There is no similar available data for Google or Azure. The number of potential beneficiaries of these certificates assumed for this analysis varies per year as follows: 1 000 experts in the first year and increasing at 10 000 after three years after which 300 experts per year.

The assumption is that each certified person typically obtains around three certifications. This reflects the average number of certificates an individual holds across different technologies or providers.

*Recurrent savings = number of people to get certified * (days saved per course * labour costs) * number of certification courses followed by a person*

Indirect savings: the effects over the economy of having a more cloud savvy and vendor-agnostic workforce are indirect and discussed in sections 6.1.4 and 6.1.5.

Sensitivity analysis: The values to be challenged in this policy measure are as follows: 1) the number of experts that can potentially be certified on a yearly basis ranging from 100 to 500 experts; 2) the certification fees ranging from EUR 50 to EUR 150; 3) the effort saved by opting for a vendor-neutral certification i,e., the number of certifications from other technologies and days saved; 4) the yearly coordination savings for the EC from avoiding duplication of effort ranging from zero to EUR 21 067 per year and 5) the total reduced costs in the certification of similar technologies from different providers stemming from the sensitivity introduced on the number of experts that could potentially get certified.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. Benefits outweigh costs systematically across the average, min and max scenarios. The min max ranges are characterised by the difference in the cost savings, and more specifically in the certification of similar technologies from different providers accounts for, as well as the number of people that can potentially be certified.

Table 38. Vendor neutral EU cloud/AI skill certificates (PM18)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	252 806	252 806	252 806	252 806

[76] https://destcert.com/resources/ccsp-certification-statistics
[77] https://aws.amazon.com/certification/

recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	-	834 269	834 269	834 269	834 269
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	285 906	-	-	285 906	47 651	714 765
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	2 301 224	2 301 224	2 301 224	2 301 224
Total costs	285 906	-	3 388 299	3 674 205	3 435 950	4 103 064
Total benefits	(78 001 031)	-	-	(78 001 031)	(18 812 153)	(122 871 064)
Net impact	**(77 715 125)**	**-**	**3 388 299**	**(74 326 825)**	**(15 376 203)**	**(118 786 000)**

3.19. PM19: Mandatory specific award criteria for the procurement of cloud and AI computing services

This policy measure has different components. First, with a view to reducing critical dependencies, this measure makes the use of the non-price award criteria under PM16 mandatory.

Public procurement represents a significant share of the EU GDP (14%) and constitutes one of the most powerful instruments available to public authorities to shape market dynamics. Traditionally, procurement decisions in the cloud sector have been governed predominantly by technical and financial criteria, such as different supported features, performance benchmarks, level agreements, and price. While these remain important, they do not present a complete picture of the sheer complexity of a cloud service. The conditions under which a service is delivered, its supply chain, hardware and software, the innovation behind it and where it is conducted, and who ultimately controls the whole chain of entities, are equally relevant, particularly for the public sector.

The competitive effect of non-technical award criteria in cloud and AI computing services procurement operates primarily through the demand side. When major public contracting authorities, notably national authorities, and large public bodies, award points for supply chain, innovation, security, interoperability, portability, and transparency, they send a clear market signal about the criteria that matter for public sector contracts. This helps to create strong incentives for providers to invest in the capabilities that score favourably, irrespective of any regulatory mandate.

Non-technical award criteria in public procurement are not just a technical adjustment to tendering practices. Used strategically and at scale, they can be an instrument of industrial and digital policy, capable of redirecting public purchasing power towards outcomes that the market, left to its own dynamics, would not spontaneously produce. In the cloud sector, where market concentration, exposure to third country laws, and strategic dependency are pressing concerns, the proposed criteria offer the mechanisms to strengthen European competitiveness, build sovereign digital infrastructure, and ensure that the public sector leads, rather than follows, the transition to a more open, resilient, and European digital ecosystem.

All the assumptions under PM16 remain valid, except in the adoption of the measure by contracting authorities that in this policy measure applies to all of them and to all tenders of cloud and AI computing services.

Administrative costs for national public authorities.

Plans. National public authorities would be required to draft and adopt a Cloud and AI development plan, covering highly critical use cases involving the purchase of sovereign services, including on how they intend to use public procurement to increase the uptake of highly innovative cloud and AI computing services. The plans shall (i) assess the value of the procurement contracts of sovereign cloud and AI computing services for critical uses cases; (ii) identify priority areas where strategic autonomy is required; (iii) monitor the procurement of innovative services, including those provided by SMEs and small-cap European providers; (iv) ensure consistency with other existing or planned national strategies. To limit administrative burden, the plan should remain concise and non-binding, focusing on priority areas, intended procurement approaches and objectives. This activity is expected to generate one-off administrative costs for public authorities, estimated as 3 FTEs per Member State (1-5 for sensitivity purposes). Member States are also expected to face ongoing administrative costs to update the strategies, estimated as 3 FTEs every 5 years.

As a follow-up, the uptake of such services, would be monitored through a centralised, Commission-led monitoring exercise (see PM21). This would create synergies with other measures within this Policy Option that are aimed at assessing the market presence of EU providers and/or existing dependencies on third country providers with respect to specific services (cfr. PM21). This activity would produce recurrent administrative costs for public authorities estimated at approximately 5 FTEs (3-7 for sensitivity) per authority.

***One-off adjustment costs for cloud and AI computing service providers*.** Providers who choose to participate in procurement processes including the specific award criteria need to align with the public procurement procedures for cloud and AI computing services. This includes adopting and aligning their processes and improving them to meet these criteria, with an estimated one-off effort of up to 20 staff days.

Recurrent administrative costs for cloud and AI computing service providers, are the costs needed to adequate the offers, assumed to be 2 staff days per bid. These days are arbitrary but were validated during the interviews as part of the supporting study. They assume only administrative work for companies who would be eligible.

The cost is calculated multiplying this effort by the number of bids presented in a year and the average salary of the cloud and AI computing service providers.

*Recurrent administrative cost = number of bids presented * effort / bid * labour costs*

Recurrent savings for cloud and AI computing service providers. Revenue gains are possible, especially for providers who can differentiate due to the award criteria. These are however not modelled.

Indirect savings: There are notable indirect benefits for cloud and AI computing service providers that are able to comply with the different non-specific award criteria. For instance, additional revenue gains, increase in reputation and the possibility to enlarge the scope of their solutions which in turn may lead to an increase of sales.

Sensitivity analysis: The impact of this policy measure is sensitive to the number of public authorities procuring cloud and AI computing services, the number of tenders and offers per year and the number of cloud and AI computing service providers and the costs to adapt the offers.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. Total costs are estimated between EUR 104 million and EUR 226 million, consisting mainly of recurrent administrative costs related to coordination, reporting, and compliance activities, alongside smaller one-off administrative and adjustment costs. Total cost savings are limited, ranging from EUR 4 million to EUR 13 million. Costs outweigh benefits across the average, min and max set of parameters. The difference in the min and max is mainly caused by the number of CSP and AI providers participating in public procurement every year across EU.

Table 45. Mandatory specific award criteria for cloud and AI computing service procurement (PM19)

Cost types	Cloud & AI providers (€)	Public authorities (€)	European Commission (€)	Total Value (central, €)	Total Value (min, €)	Total Value (max, €)
one-off administrative	-	8 333 909	-	8 333 909	3 389 039	13 480 600
recurrent administrative	53 945 915	80 878 153	-	134 824 068	94 364 632	177 304 770
one-off adjustment	3 560 007	-	-	3 560 007	3 560 007	13 708 048
recurrent adjustment	-	-	-	-	-	-
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	57 505 922	89 212092	-	146 7170984	101 313 678	204 493 419
Total benefits	-	(6 520 539)	-	(6 520 539)	(4 347 026)	(13 041 078)
Net impact	**57 505 922**	**82 6912 523**	-	140 197 445	100 049 519	213 032 412

3.20. PM20: Boosting open source in public administrations

Open source software represents a strategic policy response to vendor lock-in and the excessive dependence on vertically integrated non-EU providers. By broadening the available offer of digital solutions, open source can bridge some of the gaps left by European solution providers and reduce the public sector's reliance on large foreign technology companies for the delivery of critical services. A wider adoption of open source would also create tangible competitive advantages for EU companies, enabling them to leverage existing software building blocks and recombine them efficiently to develop and bring new solutions to market at scale.

Open source solutions can equally reduce the costs associated with digital service delivery in the public sector through use, reuse, and interoperability. When a solution is developed once and reused across multiple public administrations throughout the EU, its fixed development costs are amortised over a significantly larger user base. The creation of the EU Digital COVID Certificates illustrated this principle clearly: it demonstrated both the critical importance of interoperability for cross-border public services and the capacity of open source to accelerate deployment at EU scale. That same case also showed that open source can be a powerful vector of trust for public authorities and citizens alike.

Under this measure, public sector organisations shall take the appropriate measures to promote the use of open standards and open source software when it is equivalent or superior to proprietary one, in terms of functionalities, total cost, user-centricity, cybersecurity or other relevant duly justified objective criteria.

Under the share and reuse of open source software principle, public sector organisations shall consider the release of their software assets available for public use in an open source repository connected to the EU Open Source (OSS) catalogue. To be able to do so, the public sector organisation will have to hold the intellectual property rights. As part of the due diligence required when releasing and deploying open source software, the terms of reference should be expected to request both static and dynamic security analysis of the code, in order to mitigate risks of interference by malicious actors exploiting the publicly accessible nature of the codebase. This analysis shall be carried out by the service provider.

Public sector organisations shall not have to make their code publicly available in cases where it is restricted for reasons of national security or defence, intellectual property rights held by third parties, or due to technical or economic infeasibility.

These two principles are mutually reinforcing and should be read as complementary. Encouraging the use of open source software reshapes how digital services are planned and delivered, promoting the secure reuse of existing solutions and fostering collaboration across institutional boundaries. "Share and Reuse" is expected to expand the pool of reusable, shareable and secure software components. Together, these principles are expected to bring about a gradual, structural transformation in the way software is commissioned, produced, and maintained in the public sector.

The measure also includes the organisational and technical arrangements required to implement these principles, such as the establishment of Open Source Programme Offices (OSPOs), repositories for public-sector code, and shared infrastructure for collaboration, compliance, and training. OSPOs, as part of their role in their technical, legal, procedural and strategic – related tasks, may provide contracting authorities with advice on licenses, security, or maintenance aspects. The creation and nurturing of a Network of OSPOs would also help in further promoting, collaborating, and exchanging practices related to the use, reuse and sharing of open source, through guidance, templates or recommendations thereby sharing expertise costs across the public sector rather than requiring each OSPO to develop this capacity independently.

Overall, this measure could contribute to reduce dependencies on proprietary software products and vendors, increase public-sector use, reuse and contribution to open source, and enable efficiency and innovation gains across the European digital ecosystem. Furthermore, this measure would stimulate broader market participation, encourage new entrants, reduce vendor lock-in and improve the overall competitiveness of offers received by public authorities. Finally, it would contribute to the growth of the open source services sector in Europe, which is well positioned from increasing public sector demand for interoperable, auditable and sovereignty solutions

Open source is already the backbone of cloud services and is used in all the different layers. Without them, cloud services would not have reached the current level of technical maturity. Some examples of open source used in cloud services include:

- Infrastructure as a Service: RedHat's Open Stack is the base technology used by many European providers for the provision of Infrastructure as a Service, which is later on adjusted to accommodate to the needs of the CSPs. Open Stack allows to manage a pool compute, storage, and networking resources to build and control private and public clouds, acting as a cloud operating system.
- Data storage: Open source data bases such as MySQL, PostgreSQL or MongoDB are heavily used by cloud service providers both for relational and NoSQL databases.
- Orchestration: An orchestrator allows to automate and coordinate complex tasks across cloud environments, such as provisioning servers and storage, handling application deployments in an automated way ensuring consistency, efficiency and security. The

golden standard solution used nowadays by most cloud service providers is Kubernetes, originally developed by Google, but released as open source.

- Horizontal functionalities such as Identity and Access management as well as telemetry are also heavily implemented through the use of open source solutions. For the first, Keycloak is a relevant solution used, whereas for telemetry several solutions exist such as Grafana (for visualization), Prometheus and the Elastic Stack (ELK) and are of common practice in the industry.
- Development management lifecycle: A cloud service is mainly composed of software components that need to be architected, developed, tested and deployed. The use of open source solutions to manage the lifecycle of the service is heavily spread. For instance, for the code management and versioning, the open source GitLab is steadily growing against GitHub, owned by Microsoft, which dominates the market. Continuous integration (CI) allows companies to automate the integration of the changes and new developments made resulting in several release cycles a day. Several open source solutions for this activity exist with Jenkins CI, Travis CI and Gitlab CI being the most used. OpenAPI Swagger is also a good example of an open source solution that allows to create Application Programming Interfaces (API) to foster interoperability within the components of the application and with other applications.

The above are just some examples of how important open source is for the development and provision of cloud services. Hyperscalers also use open source software as baseline for their own solutions. As an example, AWS uses Open Telemetry[78] as the underlying technology for their solution AWS Distro[79]. Furthermore, cloud service providers, both non-EU (AWS, Oracle, RedHat) and European ones (e.g. SAP, Telefónica, Aruba, Atos, Deutsche Telekom) are large contributors to existing open source communities such as the Cloud Native Computing Foundation, which encompasses relevant projects for cloud and edge.

One-off adjustment costs for national public authorities. National public authorities will incur setup costs to establish open source repositories and the governance mechanisms defining contribution, review, and acceptance procedures. This has been estimated at 2 FTE per MS. Setting up repositories and understanding the challenges and governance mechanisms calls for a fruitful and engaging community, the assumption is that 5 repositories per MS will be initially created with an initial effort of 10 FTEs.

Nine Member States already maintain a national Open Source Programme Office or equivalent coordination structure. The measure therefore focuses on strengthening governance and coordination, aligning existing offices and governance mechanisms, and supporting those Member States that do not yet have one. For modelling purposes an assumption of additional 12 OSPOs created is taken, with a set-up cost of approximately EUR 2m. The estimates assume consistent institutional capacity across Member States, although in reality, OSPO maturity and reuse potential vary widely.

*One-off adjustment costs (NPA) = (number of OSPOs * set-up cost) + ((labour cost * effort to set-up the repositories and guidance)) * MS*

Recurrent adjustment costs for national public authorities. As software solutions developed by the public authorities are released as open source, new repositories or projects in repositories

[78] https://opentelemetry.io/
[79] https://aws-otel.github.io/

will have to be created, operated and maintained. The flagship initiative in this respect is Developers Italia that has created 408 repositories in a GitHub repository since 2017[80], averaging 50 a year but with different breadth and scope. One new repository will be created every other year. This is a very conservative assumption.

Reusing and releasing source code open source incurs into additional costs as extra quality assurance procedures must be put in place such as DevOps CI/CD pipelines, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Software composition analysis (SCA), vulnerability testing, as well processes continuously automated, and generation of the software bill of materials (SBOM) for each piece of software released and reused. This is estimated in 10 FTEs yearly per MS. The repositories shall have to be continuously maintained and governed. The assumption is that the effort dedicated to these activities increase in 1 FTE every other year, in a similar manner to the number of repositories. For this impact assessment it is assumed that all repositories created along the timespan under study will remain active. However, this is often not the situation, where repositories become deprecated due to various circumstances such as low uptake and engagement.

*Recurrent adjustment costs (NPA) = ((number of new repositories every other year * effort * labour cost) * MS) + (cost of releasing open source code * MS)*

One-off administrative costs for national public authorities stem from the adaptation of the procurement templates to the notion of promoting the use of open source software, reusable across the board for all bids. This is estimated in 30 days.

*One-off administrative costs (NPA) = (effort to adapt templates * labour costs) * MS*

Recurrent administrative for national public authorities will involve the operation of the additional OSPOs accounted for (12, as a reference number), for a recurrent cost of approximately EUR 1m per OSPO. However, certain institutional costs (e.g., existing OSPOs) are considered as marginal coordination expenses rather than recalculated in full to avoid double counting.

*Recurrent administrative costs (NPA) = number of OSPOs * cost to maintain an OSPO*

Recurrent savings for national public authorities. By reusing and adapting existing software rather than commissioning bespoke solutions, administrations can reduce duplication of effort and lower the total cost of ownership (TCO) of ICT projects. Empirical evidence[81] [82] and national case studies suggest that reuse can reduce costs by 10–40 %, depending on maturity and governance capacity.

Savings stem from the avoidance of duplication, the possibility to reuse existing solutions increasing project efficiency and the decrease of the total cost of ownership. Reusing open-source software solutions, both from other public authorities and available in open source communities results in savings mainly through the avoidance of duplication of efforts but also because the time-to-delivery of a software solution is also shortened. These have been estimated as a percentage of an average contract value of custom-built mid-software development projects, estimated at EUR 500 000. For public administrations it is assumed a cost decrease of

---

[80] https://github.com/orgs/italia/repositories?

[81] European Commission (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy

[82] Frank Nagle (2019). Government Technology Policy, Social Value, and National Competitiveness. Harvard Business School Working Paper No. 19-103.

25% due to avoidance of duplication. The rate of adoption is set to 5% for 2027 and then increasing at 2% yearly until 2036.

*Recurrent savings (NPA) = (Total cost of ownership * MS) + (savings for not duplicating the software * (Percentage of public procurement development projects addressed with OS solutions + Δ%) * number of tenders)*

Strengths and limitations of the assumptions in this policy measure

There is only a small number of reputable studies and case examples that provide inputs for the detailed parameters underpinning the assumptions, and where such evidence exists, it is often too coarse or anecdotal to support a full analysis. Consequently, the main quantitative assumptions draw on stakeholder consultations with industrial practitioners, open source communities and public administrations, conducted through interviews in the supporting study.

Despite these constraints, open source has a clearly documented economic impact. At macro level, a 2021 study for the European Commission estimated that in 2018 open source software and hardware contributed between EUR 65 bn and EUR 95 bn to EU GDP. Stakeholder consultations in the course of the study highlighted vendor lock-in as a major cost driver, with public bodies becoming dependent on single, typically US based suppliers using de facto anti-competitive practices, and one source estimating the resulting cost for European public administrations at around EUR 1.1 bn per year.

Where cost savings are concerned, the literature and case material mainly qualify effects in terms of total cost of ownership, reuse and productivity, which are reflected in the modelling of this policy option, albeit public, detailed quantifications remain scarce.

As part of the supporting study, these assumptions were cross checked with established open source organisations familiar with the costs of setting up OSPOs and the effort required to release code under an open source licence, and with public administrations that are already actively publishing open source software. In addition, the final validation workshop with software integrators, public authorities and cloud service providers was used to test and confirm several of the key assumptions.

Given the aforementioned uncertainties, this option is accompanied by a more attentive sensitivity analysis than other measures, explicitly illustrating the range of possible outcomes resulting from the variability in the main assumptions.

Sensitivity analysis: The parameters used for the sensitivity analysis include: 1) the number of the initial repositories that MS put in place at an initial stage, ranging from 5 (min and central value) to 25; 2) the effort to maintain and govern those repositories, with values moving between 0.6 FTE to 1.2 FTE, with the central value being 1 FTE; 3) the costs to set up and maintain the OSPOs, ranging respectively from EUR 2m to EUR 3m (central value is EUR 2m) and EUR 8m to EUR 28m (central value is EUR 12m); 4) the effort and contract values of the OS projects developed in and for the public administrations. Whereas the effort varies from 2 FTEs to 5 FTEs, the average contract value ranges from EUR 400 000 to EUR 600 000; 5) the total cost of ownership (TCO) and 6) the savings for not duplicating software, ranging from EUR 80 000 to 4500 00, depending on the size of the project

Indirect savings:

Open Source can have broader economic effects. When public administrations increase their procurement and use of open source software, they create additional demand for open and interoperable solutions across the wider economy. Evidence from France[83] shows that a change in public procurement rules led to measurable increases in open source activity, firm-level adoption, and software-related employment. The same mechanism, applied at EU scale, would be expected to stimulate market growth and innovation in related sectors. These spillover effects are particularly relevant at regional level, where increased public sector use of open source can strengthen local digital ecosystems and create opportunities for SMEs to participate in public procurement through open interfaces and shared repositories.

Innovation and productivity. Increased public-sector participation in open source development contributes directly to the European open source knowledge base. Studies [84,85] associate higher open source contribution rates with stronger productivity growth, faster diffusion of digital innovation, and broader SME participation in the digital economy.

Interaction model and mechanisms of impact. The policy measure operates through both endogenous and exogenous mechanisms. Endogenously, the adoption of open source first practices enhances the technological capability of public administrations. Reuse of existing code reduces project complexity and risk, while exposure to open development practices increases staff proficiency and institutional knowledge. This leads to lower operational costs and greater autonomy in managing digital systems, strengthening technological sovereignty and reducing dependency on specific vendors. Exogenously, wider public-sector use and release of open source software generates spillover effects across the domestic IT ecosystem. Local suppliers are better able to engage with open codebases and participate in collaborative development, which can lower market entry barriers, increase competition, and improve the quality of public-sector digital solutions. These dynamics reinforce each other: a more capable public administration interacts with a more dynamic local IT environment, creating a self-sustaining cycle of capability and innovation.

Results for all stakeholders aggregated and for the years covered by this measure are summarized in the table below. Total implementation costs are driven largely by recurrent adjustment costs related to setup of the OSPOs and the repositories as well as adaptation efforts. Estimated cost savings range widely, from EUR 1.6 bn to EUR 12.0 bn, depending on the realization of efficiency gains. The variation in the min and max costs from the perceived costs of the proprietary software development tools along with the savings for not duplicating the software needed.

Table 40. Boosting open source in public administrations (PM 20)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	10 389 481	-	10 389 481	6 926 321	13 852 642
recurrent administrative	-	90 711 949	-	90 711 949	60 474 632	211 661 213
one-off adjustment	-	108 623 131	-	108 623 131	56 488 617	184 117 928
recurrent adjustment	-	1 654 037 343	-	1 654 037 343	1 050 849 399	2 373 048 085
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-

[83] Orientations pour l'usage des logiciels libres dans l'administration
[84] "Free and Open Source Software and Hardware." Harvard Business School Technical Note 724-380, September 2023
[85] European Commission (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy.

recurrent enforcement	-	-	-	-	-	-	-
Total costs	-	1 863 761 904	-	1 863 761 904	1 174 738 970	2 782 679 868	
Total benefits	-	(5 251 290 954)	-	(5 251 290 954)	(1 653 692 346)	(11 955 210 083)	
Net impact	-	(3 387 529 050)	-	(3 387 529 050)	(478 953 376)	(9 172 530 215)	

3.21. PM21: Mandatory sovereign risk assessments for the use of cloud and AI computing services in the public sector

Policy Measure 21 (<u>PM21</u>) 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 **<u>shall carry</u>** out at least one sovereignty risk assessment and repeat it at least every four years or more frequently 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 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[86] or Italy[87].

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.

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 assurance). 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 States **<u>would have to</u>** 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, PM21 goes further by putting forward a framework through which the respective levels of sovereignty can be assessed.

Cloud service providers shall submit the relevant evidence that demonstrate that they comply with the sovereignty assurance criteria to the designated competent authority. For assurance

[86] See Cloud in Government Services
[87] See Strategia Cloud Italia

level 1, the service provider may issue a ‘Statement of conformity’ where they show that they comply with the cumulative criteria of this level. The cloud provider will make the statement of conformity publicly available, and shall submit it, along with the necessary evidence, to the designated competent authority. Cloud computing service providers qualifying as SMEs will not be required to undergo the validation by the national competent authority.

The assessment of the compliance of the service against the criteria for sovereignty level 2-3-4 will be performed through independent third party’s auditors. In this case, the service provider will submit the audit report and the ‘positive’ audit opinion, along with the audited evidence, to the competent authority of the country of establishment who shall verify them, without undue delay and within 60 days. The result of this activity is a draft acceptance, request for more information or rejection decision.

- In case the assessment is positive, the decision will be notified to the other Member States, who have a 60 day review period to confirm the initial acceptance conclusions by the MS of the country of establishment. During the period of review there is a recourse possibility for the Member States. If no reasoned objection has been submitted in the framed period, the validation of the audit report and audit opinion shall be considered accepted by all Member States and the service shall be recognized across the Union as a service provider that can participate in public procurement procedures across the Union. On the other hand, if reasoned objections exist, the competent authority shall assess them and decide on the maintenance or revocation of their original decision. In cases of continued objection, the Commission shall assess it. This may entail a request for additional information from the competent authorities. The Commission decision shall be binding.

- In case the assessment yields an initial rejection, the competent authority will contact the cloud provider and give the opportunity to the organization to provide comments on the evaluation. The competent authority will take into consideration these comments.

- In the case where the competent authority assesses that the submitted evidence is not sufficient, it will request the cloud service provider additional information to be provided within a certain time limit, in order to be able to issue a decision.

The competent authorities should register the decision 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 evidence proposed, but not limited to, would be modifiable by comitology. This evaluation evidence would help independent 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 assessment would be periodically renewable following the same evaluation methodology.

Policy measure 21 implies that the Commission sets up and maintains a repository of the services audited against level 2-3-4, and that public authorities assume the actual transfer cost to change from a non-sovereign service to a sovereign service (cloud porting).

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 PM15 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.

One-off adjustment costs for the European Commission

Setting up and maintaining the repository of sovereign cloud and AI computing services under the sovereignty levels. These costs include the drafting of the tender specifications for an external provider to build, develop and maintain the repository plus additional time for the evaluation and the definition of their governance procedures. This has been estimated to 120 staff days. The repository will be developed by an external contractor with a contract value of EUR 500 000.

*One-off adjustment costs (EC) = (time to draft tender specifications for the repository) * labour costs + external contract to develop the repository*

Guidelines for MS to perform the sovereignty risk assessments. In order to support Member States in the implementation of their sovereignty risk assessments, the Commission will publish guidelines. These guidelines would include the process to carry out the risk assessment, the criteria that would allow them to identify the scope, for instance by means of use cases and / or applications, the data classification process, where the market surveillance or information on sovereign services can be found. The estimated effort for the development and publication of these guidelines is 2 FTEs over 1 year.

Recurrent adjustment costs for the European Commission.

Maintenance of the repository for sovereign services. Another important activity is related to the maintenance of the repository of audited services and adjacent activities, including:

- Yearly hosting costs of the repository, estimated to be of EUR 200 000[88]. The repository will be deployed on a sovereign cloud at the Commissions' premisses and telemetry and FinOps procedures will be put in place to control expenses.

---

[88] Estimation based on the values of Simpl

- Yearly maintenance of the repository, performed by an external contractor, includes the upgrades of the software libraries amidst identified vulnerabilities, correction of errors and bugs and additional features. The estimated effort assumed for this is 2 staff days on a weekly basis.
- Oversight of the repository, including the follow-up of the contractors' activities, estimated in 2 staff days per month by the Commission staff.

*Recurrent administrative costs (EC) = costs of the yearly hosting + external contract for the yearly maintenance of the repository + (number of days for the oversight of the repository * labour costs)*

Market monitoring. In order to assess the status of the cloud and AI computing services market, the Commission will run a study for the first three years after the adoption of CADA. The goal is twofold. On one hand, it will provide input for the dependency analysis to be carried out and on the other, it will provide a deeper knowledge of the status and evolution of the cloud and AI computing services to serve for the procurement of sovereign cloud and AI services (see PM19). The limited timespan of the study is due to the following rationale: while initially this will be of importance due to, in some cases, low knowledge of existing offers, the repository and the catalogue of sovereign services would allow for a wider and deeper knowledge of the market by the contracting authorities.

This study is estimated to cost EUR 300 000 / year for three years.

***One-off adjustment costs for national public authorities*.**

Risk assessments. National public authorities and regional or federal authorities in the case of decentralized Member States are mandated to perform a sovereignty risk assessment, with the aim of mapping sovereignty assurance levels to cloud and AI computing services used in the public sector, taking into consideration aspects such as sensitivity and criticality of the data processed, risk associated to the potential unlawful access to data by third country legislation, potential disruption of the services, the service type based on a taxonomy that the Commission will publish as part of their guidance, existence of cloud and AI computing services audited under that sovereignty level, among others. The estimated number of authorities is 267, considering the NUTS-0 and NUTS-1 distribution.

The output of this result assessment will be a classification of applications or use cases categories mapped to the minimum sovereignty assurance level permitted for the procurement of cloud and AI services serving those cases.

An important element of the sovereignty risk assessment is that the existence of sovereign commercial offers will be considered as part of the exercise. This will allow to not request offers that are not available in the market or that would cause disproportionate costs to the contracting authorities as part of the procurement process.

The estimated effort for this sovereignty risk assessment is of 10 FTEs. This is a new activity for which there is yet few expertise in the Member States. It is considered that in the initial iteration, Member States will need to understand well the sectors, applications and type of data, among other aspects, that will drive their risk appetite to request one sovereignty level or another. It is expected that initially this will be an activity encompassing various ministries and agencies and therefore an intensive collaboration is expected. The guidelines from the Commission, however, should alleviate this effort.

The risk assessments will start in 2029, once EUCS and the sovereignty scheme are in place.

Designation of the competent authority, which has an estimated of 0.2 FTE per MS, which will be responsible to verify the audit reports received from the providers that had their services audited at sovereign level 2 at least.

Costs of migration to sovereign cloud by the public sector. Detailed information is provided in Annex 12 on the methodology and calculation of the costs for the migration and porting of cloud applications to sovereign cloud services.

Both the migration of the legacy-to-sovereign cloud and cloud-to-sovereign cloud applications will be performed in a linear distributed manner in a time frame spanning 5 years, starting in 2029, once there is a set of sovereign audited services.

The average cost of porting a single application to a new cloud varies from EUR 30 000 and EUR 600 000 depending on the size of the application, and not much on the type of cloud at origin or destination, as they are mainly based on human effort (400 to 8000 hours of work). See Annex 12 for an explanation of these figures.

These costs are illustrated with the real use cases in Section 6.1.2 of the main text but have not been quantified in the cost-benefit analysis, although they are described in detail in Annex 12. Since they represent planned expenditure that would be incurred in the future as part of the regular cloud contract renewal cycles and independent of the present policy measure, they have been considered outside of the cost-benefit so as not to conflate structural renewal costs with the incremental financial impact of the measure itself.

***Recurrent administrative costs for national public authorities*.**

Sovereignty risk assessment. This risk assessment shall be renewed every 4 years. The effort estimated for this reassessment of the sovereignty risks is estimated to be 5 FTEs, a lower effort than implementing the risk assessment from scratch, given that the activity is already ramped up and the Member States would already have a good understanding of their situation.

Revision of the audit reports by the competent authorities, estimated at 5 days per service audited at sovereign level 2-4. After verifying the audit report, opinion and evidence and consulting with the other competent authorities, the evaluating competent authority will adopt a decision that would allow a service provider to participate in public procurement activities.

Recurrent savings for national public authorities

Running applications on the cloud. Operating applications on the cloud, if performed well, with a continuous FinOps verifying that services are not overprovisioned can lead to significant savings. Literature sources estimate that the total cost of ownership (TCO) savings can amount to 20-50% in the case of legacy-to-cloud migrations[89]. No savings are here accounted for in the operation of applications migrated from cloud-to-sovereign cloud, as the applications would have already been benefitting from the total cost of ownership savings.

Simpler public procurement. Savings in this respect stem from the simplification of systematically using procuring audited services, which are part of the repository of sovereign cloud and AI computing services. This shall allow public administrations to save time in the verification of the documentation for the evaluation of the offer. This will result in 2 staff days

[89] Chatzithanasis & Michalakelis (2018) estimates 24% to 50% The Benefits of Cloud Computing:. Ali Khajeh-Hosseini, David Greenwood, Ian Sommerville

per bid, and assuming that there are 3.5 potential contractors presenting bids in each tender procedure.

*Recurrent savings = Average number of yearly service bids requiring sovereignty assurance level 2 – 4 * staff costs savings per bid*

Sovereign services. The savings from using sovereign services cannot be quantified due to the intangible nature of sovereignty and resilience.

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, one of the largest EU service providers of 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.

Benefit wise, cloudifying legacy on-premises services means new revenues. As to the move from traditional cloud to sovereign cloud, today's few available sovereign services come with a mark-up which is still too uncertain to draw conclusions (see discussion under Problem Driver 4 in 2.3.4). To this additional income, consulted EU service providers see also sovereign services as niche market where they have a demonstrable added value that could spill over to other market segments. The consulted companies unanimously indicated that it is too early to confirm whether, over the span of the next ten years, the incremental cost and benefits would reach the same balance (i.e. margins) as with equivalent non-sovereign services, which is today commonly assumed to be around 30%[90]; to cater for this uncertainty, this assessment assumes that stakeholders' margins vary from 25% to 35%.

[90] Amazon Web Services profits squeezed as AI arms race drives spending surge – GeekWire

One-off adjustment costs for cloud an AI computing service providers

Ultimately, the decision of a provider to subject to the sovereignty assessment one or more services is their own business decision. However, in order to have a sense of magnitude of how many providers could be affected by the sovereignty scheme and based on extensive desk research conducted as part of the preparatory study (Technopolis et al., 2025), it was identified that services from 59 non-EU headquartered cloud service providers meet Level 1 requirements and would be able to qualify to Level 2 should they decide so. 226 EU headquartered providers could qualify their services as Level 2 and would be able to qualify their services as Level 3 should they decide so. If only large companies are considered and SMEs are excluded, the figure goes down to 59 EU headquartered large companies.

The assumptions are as follows: 600 services will be audited from 2029 until 2034, with the assumption of 30 audits the first year, and an annual growth of 82%. This builds over the number of services currently qualified in comparable national qualification and certification schemes[91], and the FedRAMP mechanism. As of September 2025. the FedRAMP repository contains 530 authorised services under level moderate and high.

Audit: Services may be audited under different assurance levels, provided that the criteria mentioned above (see PM11) are met. For the purpose of this impact assessment, it is estimated that the proportion of services that get a positive audit report across the different assurance levels will be mirroring the needs of the public authorities (see below). This would then make that out of the estimated 600 sovereign cloud services [92]:

- 70% of the services will be Sovereignty Assurance Level 1, making 420 services
- 20% of the services will be Sovereignty Assurance Level 2, resulting 120 services
- 9% of the services will be Sovereignty Assurance Level 3, amounting to 54 services
- 1% of the services will be Sovereignty Assurance Level 4, resulting in 6 services.

The effort needed to get audited as sovereign under the sovereignty assurance level 2 -4 is estimated to be 15 FTEs. This includes the definition and implementation of the necessary legal, organisational and technical measures to reach sovereignty assurance level 2 – 4 and the auditing procedure carried by the third party auditor. This effort was validated in the Final Validation workshop held as part of the study led by Technopolis.

*One-off adjustment cost of new audits (CSAP) = (effort to get audited sovereignty assurance level 2 – 4 * labour costs) * number of audited services assurance level 2 – 4*

One-off regulatory fee for cloud and AI computing service providers

*New audits***,** the fee is assumed to be EUR 20 000, for the estimated number of services awarded sovereignty assurance level 2– 4.

*One off regulatory fee for new audits (CSAP) = regulatory fee * number of services sovereignty level 2 – 4*

Recurrent regulatory fee for cloud and AI computing service providers

Renewal of audits: fee is assumed to be EUR 14 000..

[91] For this impact assessment ES, IT, and FR have been considered as baseline as their data is public.
([92]) see footnote 90

*Recurrent regulatory fee for new audits (CSAP) = regulatory fee * number of audited services assurance level 2 – 4*

Recurrent administrative costs for cloud and AI computing service providers

Audits: These compliance costs stem from the audits . to maintain the positive audit report, where the goal is to verify that the conditions under which the sovereignty level was obtained remain valid (effort estimated as 3 FTE/year per service). Compared to the effort needed to achieve the award of a sovereignty level, the effort dedicated to the intermediate audits has been assumed to be lower than obtaining the initial qualification, in spite of the annual reporting obligations set out above.

*Recurrent administrative compliance cost of sovereignty level renewal = (time to be audited * labour costs) * number of services sovereignty level 2 - 4*

Recurrent savings for cloud and AI computing service providers

Audits. A crucial matter in the analysis of the recurrent savings for cloud and AI computing service providers is the single market effect especially considering the mandatory nature of this policy measure. Providers will be able to audit their services in one MS and be able to offer them in public procurement procedures in all EU-27. The analysis assumes that in the business-as-usual scenario one cloud service provider would seek to run the audit for one service in 10 MS to be on the conservative side. Given the costs of compliance, in a business-as-usual case, a cloud and AI computing service provider would carefully prioritize in which MS(s) it would seek to obtain a similar audit of a service usually taking into consideration aspects such as the market share or other commercial opportunities.

*Saving costs audit valid throughout the EU = Number of MS where the Cloud and Service Providers would get audited * cost to get audited * number of audited services assurance level 2 - 4*

Public procurement. Another relevant saving stems from the fact of not having to collect and resubmit all the evidence necessary to demonstrate that the criteria are fulfilled for each bid, given that the certified services are listed in the repository and accessible for the contracting authority. The assumption is that undertakings will save 2 staff days / year per service and bid. The number of yearly bids amounts to 50 a year.

*Business costs saved: = Businesses time saved per evidence submission in a tender procedure * number of submitted bids*

Recurrent administrative costs for the private sector (Auditors)

Third party audits. In this PM, as mentioned above, the target number of cloud and AI computing services audited as sovereign is estimated to reach 600 by 2032[93], whereas 30 of these will reach sovereign level 2-4 during the first year. The assumed CAGR is 82%. The assumption under this policy measure follows a linear progressive uptake of the audit scheme.

The estimated average effort for auditing a service under Sovereignty assurance level 2-4 is 110 days / audit. The same effort is considered for the renewal process.

[93] Assumption taken considering the current valid authorised cloud services in FedRAMP moderate and high, which amounts to 531 as of 26 September 2025.

Recurrent administrative costs for the private sector (Private sector essential entities operating in sector listed under NIS2 Annex I)

Risk assessment. These are the costs incurred by essential private sector entities listed as under annex I of NIS2 to sovereignty related risks in their current risk assessments. The effort estimated is 60 staff days per essential entity for the first year and 12 staff days for the following ones to account that the novelty generates larger work that re-doing it.

The SWD published as part of the proposal for the Digital Omnibus [94] estimates that the number of all entities, essential and critical, from the private and public sector, affected by NIS2 Annex I amounts to 160 000. France's NIS2 available data, indicates that 20% of its entities are classified as essential entities under Annex I, with the remaining 80% designated as important entities under Annex II[95]. Re-using the same ratio for the EU implies 160 000 * 20% = 32 000. To which the private sector is assumed to represent 80%, or 32 000 * 80% = 25 600.

Indirect savings: Similarly to PM15, through this measure, cloud and AI computing services able to adequate their processes to comply with the audit scheme will increase trust from public administrations, and notably for the use cases identified as need-to-be sovereign based on the sovereign risk assessments performed. This will result in more trustworthy, credible and very specialized as well as very advanced offers responding to challenges such as resilience and autonomy. Given the mandatory nature of this PM, the indirect savings are expected to be larger in this measure than in PM15.

Sensitivity analysis: The most affected parameters for this Policy Measure are as follows: 1) the effort needed by a cloud and AI computing service provider to obtain the audit; 2) the number of MS where cloud and AI computing services would seek the audit in the absence of a single market; 3) the initial number of cloud and AI computing services audited during the first year and the annual growth; 4) the number of submitted bids per year; 5) effort by the private sector for the risk assessments, 6) effort by public authorities for the risk assessments.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. The main source of variation in the min and max comes from the cost savings, and notably the savings from the EU-wide validity per service for cloud and AI computing service providers and the number of countries where providers would audited/validated, in the event the scheme would not exist.

Table 41. Mandatory sovereign risk assessment for the use of cloud and AI computing services in the public sector (PM21)

Cost types	**Private sector**	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-	-
recurrent administrative	1 439 144 597	80 856 542	562 624		1 520 563 763	540 444 577	2 763 406 090
one-off adjustment	-	254 272 125	154 624 928	693 692	409 590 745	247 443 239	571 738 249
recurrent adjustment	-	-	68 603 894	2 965 857	71 569 751	44 128 193	44 128 193
one-off regulatory fees	-	3 022 890	-	-	3 022 890	3 022 890	3 022 890

[94] SWD(2025)836 final
[95] Cybersécurité : la transposition de la directive NIS 2 examinée le 11 mars au Sénat

recurrent regulatory fees	-	3 367 639	-	-	3 367 639	3 367 639	3 367 639
one-off enforcement.	-	-	-	-	-	-	-
recurrent enforcement		-	-	-	-	-	-
Total costs	1 439 144 597	341 519 196	223 791 446	3 659 549	2 008 114 787	838 406 538	3 385 663 062
Total benefits	-	(3 349 440 466)	(2 507 623)	-	(3 351 948 089)	(1 676 992 882)	(5 085 107 859)
Net impact	1 439 144 597	**(3 007 921 270)**	**221 283 823**	**3 659 549**	**(1 343 833 301)**	**(838 586 344)**	**(1 699 444 797)**

This policy measure would trigger an acceleration of porting of some applications to sovereign cloud services of assurance levels 2 to 4, requiring an anticipation of expenses of EUR 3 to 15 bn. These costs are estimated and reported under section 12.4 of Annex 4. Since they represent planned expenditure that would be incurred in the future as part of the regular cloud contract renewal cycles and independent of the present policy measure, they have been scoped outside of the summary cost table so as not to conflate structural renewal costs with the incremental financial impact of the measure itself.

The benefits accruing from the risk reduction, notably an increased autonomy and strengthened operational resilience through the adoption of sovereign cloud and AI computing solutions are intangible and cannot be expressed in quantitative terms. While these benefits cannot be quantified, they are acknowledged as a significant consideration underpinning the policy rationale.

3.22. PM22: EU-level Procurement of cloud and AI computing services

PM22 builds on top of PM17, establishing in addition a framework for the public procurement at EU-level of data centre, cloud and AI computing services.

Cloud Capacity in the Public Sector. Same assumptions as in PM17 are taken for all impacts related to the public sector cloud federation. Same number of public authorities at all levels participate in the public sector cloud federation.

Joint Procurement. The Union procured 2,5 trillion EUR in services in 2024, from 250.000 public authorities[96]. Section 2.4.3 ("Public procurement contract values for cloud and AI computing services") of this annex shows that cloud and AI computing services represented 0,68% of the total services procured by the public sector in Europe in 2024. The value of cloud and AI contracts procured by the public sector in that year (0.68% x EUR 2,5 trillion = EUR 17 bn) is projected to the future using the CAGR observed in the period 2021-24 (20%) for the first years up to 2030 and a half of that from then on.

A progressive roll-out of the EU-level joint procurement is considered, starting at 2% of the procured service volume (EUR 340 m) and increasing by 2 additional percentage points every year, reaching 22% at the end of the 10-year period (EUR 21 bn). The level of savings will also increase over time as higher volumes are aggregated, and experience is gained, starting at 10% and growing annually by 4 additional percentage points till 2032, reaching 30% in that year.

One-off adjustment costs for the European Commission include those related to set up the platform for federation, procurement, brokering and service aggregation. These costs include 4 persons half time in 2027 (2 FTE) from the Commission to run the procurement process for the

[96] From Public Procurement Data Space: https://www.public-procurement-data-space.europa.eu/en

platform (define requirements and prepare the call, assess and refine the proposals and award the contract), that will be tasked to a subcontractor for development and deployment at an estimated cost of EUR 40 000 000. This figure represents additional EUR 20 000 000 with respect to the federation platform considered in PM17 to cover the service repository, procured service catalogue and brokering and service aggregation functionality.

One-off adjustment costs = Platform costs + EC Staff costs for platform procurement

Recurrent adjustment costs for the European Commission relate to hosting the platform in a cloud, estimated at 1.5 million EUR per year, operating, maintaining and evolving the federation platform, with an effort of 100 contractor FTEs per year (40 additional to those required in PM17 to cover the extended functionality). The Simpl programme has been used as a reference for the underlying costs assumption[97] .

Recurrent adjustment costs = Hosting + Maintenance & Integration contractor costs

Recurrent administrative costs for the European Commission, stem from the costs to manage the cloud federation and the operation of the joint procurement process. In addition to the resources of PM17 to set up the public sector cloud federation, a further 12 FTEs are dedicated in 2027 to design and setup the joint procurement framework.

On a yearly basis, in addition to the resources estimated in PM17 to manage the cloud federation, a further 20 FTEs are dedicated to run the EU-level procurement processes.

Recurrent administrative costs for the European Commission =
costs to manage the federation + operation of the joint procurement process

One-off and recurrent adjustment costs for national public authorities. The Public Authorities dedicate the same effort as in PM17 to participate in the setup of the public sector cloud federation, and to connect the infrastructures and keep updated the characteristics of the shared resources in the federation platform.

Recurrent savings for national public authorities. Recurrent savings from federation, coming from reducing idle capacity, getting cheaper computing resources and reducing the coordination effort for sharing cloud, are the same as in PM17.

With regards to the procurement of cloud and AI computing services, it is assumed that each Public Authority dedicates an average of 3 FTEs. Thanks to joint procurement, 0.5 FTEs are assumed to be saved in the procurement process in each of the Public Authorities. The demand aggregation and service composition provided by the service platform will save additional 0.5 FTEs per Public Authority, coming from buying more efficient pre-integrated solutions.

The participation in the joint procurement framework and the aggregation of demand in the common EU-level procurement process will produce 2 effects: a reduction in the FTEs required for procuring cloud and AI computing services (see above) and a reduction in service prices coming from higher scale, purchase power.

[97] Simpl: Cloud-to-edge federations empowering EU data spaces

Recurrent savings = saved effort in PAs x NPA staff cost x number of PAs + cloud and AI computing service procurement volume x % procured at EU-level x % discount

The share of cloud and AI computing services procured at EU-level and the discount achieved by aggregating demand at EU-level grow over the years at the rate described above in this section.

Indirect savings: The increase in public procurement of cloud and AI sales volume that is addressable by European providers may help to increase their scale and competitiveness and their share in the European and global cloud and AI markets. Joint procurement and federation can also help in accelerating cloud and AI adoption in public administrations thanks to the reduction in service costs.

Sensitivity analysis: The results have been challenged in terms of savings for national public authorities namely: 1) Yearly administrative time saved thanks to fewer coordination needs for national public authorities; 2) FTEs saved thanks to joint procurement – yearly; 3) Savings in terms of effort incurred by participating PAs due to the possibility to aggregate demand and compose services - yearly; Considering IaaS + PaaS + SaaS, deployment automation. Midsized application. All values were set to range between a min of 0.1 to a max 0.5 FTEs corresponding to a min of 22 days to a max of 110 days; 4) capacity shared by each MS with the federation ranging from 5% to 15% which impacts the savings in terms of idle capacity reduction.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below. In all scenarios including the average, min and max savings outweigh costs. The main source of variation in the min and max comes from the cost savings, and notably the savings in terms of idle capacity reduction.

Table 42. EU-level Joint cloud and AI Procurement (PM22)

Cost types	**Cloud & AI providers** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-		18 689 579	18 689 579	18 689 579	18 689 579
one-off adjustment	-	4 613 563	40 009 806	44 623 369	44 623 369	44 623 369
recurrent adjustment	-	213 669 483	163 981 548	377 651 032	334 125 766	421 176 297
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	-	218 283 046	222 680 933	440 963 980	397 438 715	484 489 245
Total benefits	-	(34 199 254 362)	-	(34 199 254 362)	(19 170 613 237)	(49 227 895 486)
Net impact	-	**(33 980 971 315)**	**222 680 933**	**(33 758 290 382)**	**(18 773 174 523)**	**(48 743 406 241)**

3.23. PM23: Financial support for SMEs to adopt cloud and AI

This policy measure puts forward a targeted scheme to provide financial support to SMEs for adopting cloud and AI computing services to increase their productivity and competitiveness. A yearly budget of EUR 40 050 000 is considered over the 10-year period. This is done for modelling purposes only and does not pre-empt the next MFF:

- Most of it, EUR 38 500 000, is dedicated to supporting the design and planning phase of cloud and AI-based transformation projects for SMEs.
    - The grants are fixed amounts that the SMEs can spend in consultancy services to design digital transformation projects based on cloud and AI technology.
    - The amount will depend on the size of the SME: small SMEs (10 to 50 employees) will receive EUR 10 000 and midsize SMEs (50 to 250 employees) EUR 25 000.
    - The grants can be spent in services from a catalogue of self-published organizations maintained by the Commission that will include consultancy service providers from the IT sector in all MS. The catalogue would be populated based on an objective and transparent process.
    - The objective is reaching 2% of the small (10 to 50 employees) and midsize (50 to 250 employees) SMEs over the 10-year period.

- Every year, the SMEs that have designed the most innovative cloud and AI-based transformation project plans will receive additional support to fund their implementation:
    - small SMEs would receive EUR 100 000 each.
    - midsize SMEs would receive EUR 250 000 each.
    - Total yearly budget for awards would be EUR 1 050 000.
    - A jury will assess the project plans designed every year and select the ones to be awarded.

- The rest, EUR 500 000, serves to communicate and create awareness of the programme, and disseminate the results, giving visibility to the most successful and innovative project to serve as relevant references that may inspire SMEs across the different sectors and MSs:
    - The awards will be communicated and made visible through reports, social media, and events, and the project descriptions will be made available in a web site to serve as references.
    - The awards will reward innovation and its transformation impact in terms of efficiency, productivity and competitiveness.
    - There will be a balanced distribution of the awards among sectors and MSs, so that relevant references are created across all markets.
    - An SME project assessment team will define specific criteria for awarding the grants and select the awarded SMEs out of the presented proposals. The calculation of the evaluation efforts considers that there are 5 proposals presented for each awarded grant.

The SME Performance Review report shows that there are 26.1 million SMEs in Europe, out of which 24.5 million are micro enterprises (less than 10 employees), 1.4 million are small enterprises (10 to 50 employees) and 214,000 are midsize companies (50 to 250 employees). The cloud adoption scheme applies to small and midsize enterprises, with the objective of reaching 2% of each category in the 10-year period. This means a total of 32 200 companies engaged, 28 000 small ones and 4 200 midsize ones, will be direct beneficiaries.

The awarded SMEs will use the award to contract consultancy services from a catalogue provided by the Commission that will contain service providers from different MS and diverse profiles. These providers will be mostly local IT SMEs with skills in cloud and AI technology, that will be indirect beneficiaries from this policy measure.

Eurostat reports 1 281 000 businesses in the ICT sector[2], out of which 820 800 are dedicated to computing, consultancy and related services. From Eurostat's database[3], the number of micro companies (less than 10 employees) in the ICT sector is 1 220 000 (as of 2020), 53 000 are small (10 to 50 employees) and 12.000 are medium size (50 to 250). The catalogue of digital consultancy service providers will contain some of the European small and midsize IT enterprises (66.8% of the ICT sector, 43 420 companies in EU) that have the right skills and resources. Assuming that each service provider manages 5 consultancy projects along the 10-year period, the policy measure could indirectly benefit 6 440 IT SMEs that would support the awarded SMEs in their project design and planning.

One-off and recurrent administrative costs in the European Commission. The Commission will apply an effort of 1 FTE for the design and set up of the cloud and AI adoption programme, requiring consultation with stakeholders (Member States, associations and SME representatives) and the elaboration of the programme description. The infrastructure required to run the programme, manage the calls and monitor its execution would re-use existing infrastructure and is accounted for here. The cost of the catalogue and the onboarding of IT consultancy service providers are considered negligible.

On a ***recurrent basis,*** the Commission will need 100 staff days to administer the cloud and AI adoption programme, including the preparation, launch, management and closing of the different calls, and 0.6 staff days to assess each of the proposals presented. The grants will amount for EUR 10 000 and EUR 25 000 for small and mid-sized SMEs respectively.

One-off administrative costs in SMEs. The effort to prepare a project proposal is estimated to be 2 persons for 10 days (20 staff days). A sensitivity check for this parameter is accounted for.

Cost savings in SMEs. The benefits stem from the design of the projects supporting the AI-based transformation. The percentage of small and mid-sized companies benefitting respectively from the EUR 10 000 and EUR 25 000 grant is 2%.

Indirect savings: the expected increase in the adoption of cloud and AI computing services in European SMEs from different sectors resulting from this initiative is discussed in section 2.5.5 of this annex.

Sensitivity analysis: The policy measure depends mainly on the targeted reach (% of benefitted SME).

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below.

Table 43. Financial support for SMEs to adopt cloud and AI (PM23)

Cost types	**SMEs** (€)	**Public authorities** (€)	**European Commission** (€)	**Total Value** (central, €)	**Total Value** (min, €)	**Total Value** (max, €)
one-off administrative	55 373 982	-	84 269	55 458 251	27 725 295	83 443 215
recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	-	-	-	-	-
recurrent adjustment	-	-	339 317 286	339 317 286	171 954 564	509 704 787
one-off regulatory fees	-			-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	55 373 982	-	339 401 554	394 775 537	199 679 859	593 148 002
Total benefits	(328 412 809)	-	-	(328 412 809)	(164 206 405)	(495 604 785)
Net impact	**(273 038 827)**	-	**339 401 554**	**66 362 727**	**35 473 454**	**97 543 217**

3.24. PM24: Tools to enrich EU cloud and AI computing services offering

This policy measure sets up actions to improve the competitiveness of European cloud and AI computing services by facilitating tools to improve their service offer and meet the demand for cloud and AI computing services in different sectors. The aim is to a) promote the development of open source tools that allow to combine, compose and integrate diverse functionality to deliver more complex services and ease their consumption, deployment and operation (the "Toolbox"), b) make visible these tools and other open source software components for cloud and AI computing services in a repository at Union level (the open source Cloud and AI "Repository").

The Repository will improve their visibility and accessibility to the cloud and AI service provider community, and the Toolbox will facilitate smaller providers to enrich and enable a more integrated and competitive offer of cloud and AI services, reducing the functionality gap with the rich marketplaces provided by the dominant players.

One-off administrative costs for the European Commission. The Commission will dedicate 0.5 FTEs during the first year to design the programme(s) for the development of Toolbox components.

Recurrent administrative costs for the European Commission. 0.5 FTE is estimated to manage every year the repository, review and monitor the programme(s) and run administrative, compliance, financial, communication and community engagement work associated to the Toolbox development and the open source Repository.

One-off adjustment costs for the European Commission. The Commission will allocate 500 000 EUR as one-off cost for building the cloud and AI service toolbox repository and will dedicate 0.5 FTEs to procure it and set it up.

Recurrent adjustment costs for the European Commission. The EC will engage an external contractor to maintain the service repository with each year 1 FTE. The EC will host the platform with a yearly cost of 100 000 EUR.

A community of cloud and AI computing service providers, software and technology providers, cloud and AI consumers from different sectors, research organizations and public sector organizations will be set up to help in defining requirements and objectives for the development programmes and for the repository, and provide feedback about the results to steer them properly.

Indirect savings: the expected benefit is an qualitative improvement of the offer of Cloud and AI computing services from European providers that will increase the competitiveness of their portfolios and help them gain market share and scale. The open source nature of the developments will also contribute to the compatibility, interoperability and portability of solutions among European cloud and AI service providers, improving the freedom of choice for customers and competition. Due to the community nature of the development, it will also increase innovation by allowing contributions and reach for small companies and individuals.

Sensitivity analysis: The benefits are only presented from a qualitative perspective.

Results for all stakeholders aggregated and for the years covered by this measure are summarised in the table below.

Table 44. EU cloud and AI toolbox (PM24)

Cost types	Cloud & AI providers (€)	Public authorities (€)	European Commission (€)	Total Value (central, €)	Total Value (min, €)	Total Value (max, €)
one-off administrative	-	-	-	-	-	-
recurrent administrative	-	-	-	-	-	-
one-off adjustment	-	-	542 134	542 134	542 134	542 134
recurrent adjustment	-.	-	2 364 883	2 364 883	1 938 373	2 791 393
one-off regulatory fees	-	-	-	-	-	-
recurrent regulatory fees	-	-	-	-	-	-
one-off enforcement.	-	-	-	-	-	-
recurrent enforcement	-	-	-	-	-	-
Total costs	-	-	2 907 017	2 907 017	2 480 507	3 333 527
Total benefits	-	-	-	-	`-	-
Net impact	**-**	**-**	**2 907 017**	**2 907 017**	**2 480 507**	**3 333 527**

4. Strengths and limitations of the analysis

This impact assessment uses as main basis the results and the modelling stemming from the study carried out by Technopolis Group. In spite of extensive efforts to collect relevant data through surveys, interviews and workshops certain gaps remain. There are a number of points for which projections and estimates had to be considered. For instance, there is no clear objective value on the deployed data centre capacity in the EU. The study carried out by Technopolis et al. (2025) has developed a first-of-a-kind methodology to estimate current capacity in the EU, which has then cross-referenced with reported literature sources. As for the international comparison, several reports on US data centre capacity exist, but the numbers for China are not so conclusive.

The estimation on the use of energy and water currently used by data centres present similar issues. The reported values stem from literature sources. Both the data centre capacity figures as of today as well as the growth scenarios have been thoroughly assessed with one-to-one interviews, CATI interviews and in the two workshops organized along the timeframe of the study.

Determining the market size for cloud and AI computing services remains methodologically heterogeneous. Sources differ notably because they don't look at same layers (IaaS, PaaS or SaaS) or don't aggregate them the same way (e.g. IaaS and PaaS, or IaaS-PaaS-SaaS), resulting in partial overlaps and limited comparability across studies. As a consequence, the figures presented here should not be read as precise point estimates. To mitigate these limitations, a triangulation of these estimates across multiple sources was performed, validating the ranges to establish a robustness check.

There is also no hard evidence with respect to the number of public authorities procuring cloud and AI computing services, nor on the contracts awarded or the number of IT systems that are either cloud-aware or cloud-native. The data base from Tenders Europe Daily (TED) has been taken as the baseline since it contains all the notices published in the supplement of the Official Journal of the European Union. However, not all contract services are published on TED – only those surpassing a certain value, namely EUR 143 000 for central governments and EUR 221 000 for local and regional governments are required to be published. Furthermore, the absence of a distinct code under the common procurement vocabulary for cloud and AI computing services required a complex query using combinations of keywords. This poses some limitations in the completeness of the data. Other aspects considered in the impact assessment such as the federation of resources or the sovereignty risk framework, for which little hard evidence exists due to their novelty, were based on existing pilots (e.g. Simpl[98]) along with interviews to public administrations and cloud and AI computing service providers to verify the validity of the assumptions. These were further verified in the final validation workshop organized the Technopolis Group with stakeholders from different profiles.

It is also important to note that the direct cost and cost savings/ benefits identified in the analysis for the Policy Measures under Section 3 above do not incorporate wider economic impacts, which have been excluded due to limitations in available data for monetising these effects. Therefore, the results above, do not represent a comprehensive assessment of total policy value, but should rather be interpreted as partial estimates of efficiency of each policy measure for the stakeholders under consideration.

Finally, wherever there was a gap that could not be covered through interviews, CATI surveys, or literature, the study team drew reasonable assumptions. These assumptions have been tested in the final validation workshops, which helped provide elements to confirm or adjust these assumptions. In the event these unknown parameters played a pivotal role in the assumptions, the contracting team applied a min-max approach to demonstrate the robustness of the data.

5. Sensitivity Analysis

A scenario-based sensitivity analysis was run to understand the CBA model output behaviour in response of changes of its inputs to evaluate its overall stability and reliability. It was conducted to verify the uncertainty range (confidence interval) of the values estimated in the CBA for the most impactful policy measures. A *min* and *max* variation for the parameters was introduced to create word and best case scenarios for each measure. The parameters that were varied have been selected according to the following logic:

- When the formulation of the parameter involved a high degree of arbitrary assumptions, e.g. time savings due to administrative simplification.
- Due to the parameters' highly volatile nature: for example, the number of proposals submitted per year or the cost for a software application. To be noted that this variability does not only reflect the size of the company / public authority affected (that is modelled separately), but captures elements that are not easily separable, such as different organisational or business model choices.
- When stakeholders reported during interviews minor to no costs or costs savings the min. value is set to zero, while the maximum value is the parameter identified according to other assumptions (i.e. stemming from the literature or other expert assumptions).

It is important to underline that the sensitivity analysis presented here provided a bounded variation assessment, through which each policy measure has been tested under a minimum and maximum scenario. As the measures differ considerably in their design, target audience, and the type of impacts generated, the variables are not always uniform or comparable. Therefore, the min-max range is not to be interpreted as a consistent sensitivity interval across all measures. The objective of the exercise was to understand how their costs and benefits would have varied under minimum and maximum conditions, when the most influential assumptions are varied within plausible ranges. This has allowed to assess the stability of each

[98] The second specific contract for Simpl includes a technical feasibility analysis to assess a federation of cloud resources across several Member States. More information: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/14888

measure's performance across a realistic range of assumptions. The variation was based on evidence coming from interviews, observed practice and feasibility considerations. The Table below presents the scenario-based ranges for each policy measure, which capture the uncertainty stemming from changes in key parameters and assumptions varied jointly under best and worst case scenarios.

Individual net benefits/costs of the measures expressed in NPV over 10 years can be seen under each Policy Measure in Section 3, as the main indicators of the net value of each measure. The results and interpretation, presented in the table below, show that most PMs exhibit strong robustness across all tested ranges, with net positive impacts even under pessimistic conditions.

Table 45. Interpretation of the parameters used for the sensitivity analysis

Policy Measure	Key Parameters varied	Central NPV and scenario range (€ m)[99]	Result and interpretation
PM3: Adopting guidelines on building sustainable data centres in the EU	• Adoption rate of guidelines by DC projects (30%-70%) • Time saved per project for operators (5-15 days) • Time saved per project for authorities (5-15 days) • Adoption effort by operators (10-30 days)	5.8 [-3.6 – -11.7]	PM3 delivers net costs in both min and max scenarios, as administrative efficiencies and reduced operator/authority workload are not sufficient to match the adoption effort by operators and authorities. Results are sensitive to assumptions, with outcome ranges exceeding 100% of the central estimate, indicating uncertainty around magnitude.
PM4: Project facilitators for the roll-out of data centres	• Time saved in permitting processes (4-8 months) • No. of DC projects benefitting from this PM by 2036 (30%-70%) and proportionately the previous years. • Implementation costs for authorities (3-5 FTEs) • Time savings by authorities (10-20 days)	4 617.6 [1 859.9 – 8 632.9]	PM4 generates net savings, which increase significantly under the max scenario, where more projects benefit, and time savings are larger. This shows that the measure becomes increasingly efficient when permitting time reductions scale. Estimates vary widely across assumptions, with a relative spread of at least 100%, implying moderate confidence in direction but limited precision.
PM5: Mechanism for Member States to identify areas to fast-track data centre deployment	• Time saved in permitting processes (6-10 months) • No of DC projects using the areas by 2036 (30-70%) and proportionately the previous years. • National authorities' effort to set up and administer the new process (1-8 FTEs/year) • Energy efficiency (PUE, i.e. amount of data centre power dedicated to IT).	11 861.4 [6 158.1 – 18 874.9]	PM5 provides large net benefits, which grow considerably when more new DC facilities use fast-track areas or when more months are saved. All scenarios show net benefits, although large differences between best and worst-case outcomes (≥100%) point to relevant scenario dependence.
PM6: National funding support for data centres	• National authorities' effort for setting up and administering the funding scheme (2-4 FTEs) • Number of MS administering the scheme (25%-75%)	-10.8 [-3.7 – -21.2]	PM6 represents an adjustment and administrative cost for public authorities and operators. Given the voluntary nature of the scheme, no benefits are available or quantifiable. The costs are expected to increase

[99] NPV refers to the net present value of benefits minus costs. Positive values indicate net benefits; negative values indicate net costs.

Policy Measure	Key Parameters varied	Central NPV and scenario range (€ m)[99]	Result and interpretation
	• Business efforts to respond to the calls/prepare an application (35-55 working days) • No. of proposals submitted every two years (6-18)		moderately in the max scenario due to higher efforts and MS administering the scheme. Considering potential policy impacts, these cost variations could be considered not very sensitive to changes in assumptions. Best- and worst-case results diverge (≥50%), suggesting moderate robustness with scenario-sensitive magnitude.
PM7: Set deployment targets and monitor progress	• Time needed per operator to participate in the monitoring exercise (0.5-1.5 days/year) • Time needed by authorities to participate in the verification of data (2-4 working days) • Time and resources needed by the Commission to set up and manage the monitoring (1-2 FTEs and 20-30 days per year)	- 2.3 [-1.7 – -2.8]	PM7 reflects only administrative and adjustment costs, with benefits being largely indirect (e.g. improved monitoring, market transparency). Costs increase slightly with higher participation or expanded monitoring roles. Sensitivity is limited and cost impacts remain modest when compared with other PMs. Net costs are consistently observed across scenarios with limited variation, indicating high robustness.
PM8: EU funding for R&D and innovation ecosystems for cloud and AI	• Total effort for the Commission to administer the scheme, i.e. set-it up (2-4 FTEs) and manage it periodically (1-2 FTE) • Business efforts to respond to the calls/prepare an application (35-55 working days) • No. of proposals submitted every two years (16-24)	- 2.2 [-1.4 – -3.1]	PM8 generates adjustment costs for the Commission to set up and manage the scheme and administrative costs for businesses applying to receive possible funding. Given the uncertain nature of the possible funding, benefits have not been monetised. Thus, this PM appears only as a cost measure. Overall costs remain relatively low with respect to other measures. All scenarios indicate net costs, but differences between outcomes exceed 50%, yielding high confidence in direction and moderate confidence in magnitude. The range reflects the variation in staff needs and effort, based on eventual proposal and funding volumes.
PM9: EU deployment funding for strategic projects	• Total effort for the Commission to administer the scheme, i.e. set-it up (2-4 FTEs) and manage it periodically (1-2 FTE) • Number of proposals every two years • Business efforts to respond to the calls/prepare an application (35-55 working days) • No. of proposals submitted every two years (11-19)	-1.9 [-1.2 – -2.7]	Similarly to PM8, PM9 includes only administrative and adjustment costs for key stakeholders. As in PM8, sensitivity is relatively low to the varied parameters. Net costs occur across scenarios, with moderate dispersion (≥50%) between outcomes. Costs increase with higher proposal volumes and staffing assumptions.
PM10: EU-level identifications of areas to fast-track data centre deployment	• Time saved in permitting processes (2-4months) • No of DC projects using the areas by 2036 (30-70%) and proportionately the previous years.	7 979.7 [4 663.8 – 12 114.0]	Similarly to PM5, PM10 generates large net savings due to the benefits brought by earlier commissioning and operational efficiencies, multiplied by the new DC projects that would benefit from this measure, under the specific growth scenario.

Policy Measure	Key Parameters varied	Central NPV and scenario range (€ m)[99]	Result and interpretation
	• National authorities' effort to participate (5-15 days/year) • Cost savings for authorities (0.5-1.5 FTEs/year) • Energy efficiency (PUE, i.e. amount of data centre power dedicated to IT).		Net benefits are robust across scenarios, though assumption-driven variability above 50% reduces precision, yielding medium–high confidence overall. The PM is sensitive to months saved and PUE levels. The latter significantly influences overall OPEX. NPV increases by around €1.1 m per month of time saved and by €0.7 m for every 0.01 improvement in PUE.
PM11: Creating a EU-level harmonised criteria for sovereign cloud and AI computing services	• Number of procuring authorities (50% - 100%) • Share of procurement procedures that will voluntarily request the alignment with the definition of sovereignty (5% - 10%)	0.3 [0.2 – 0.4]	PM11 shows a moderate level of sensitivity with the max scenario double the min one. Net benefits are observed consistently across scenarios and assumptions, with limited dispersion, indicating high robustness. However, the absolute scale remains small, indicating that even if assumptions vary the overall impact of this PM is limited in economic terms.
PM12: Creating EU guidelines for sovereign cloud and AI computing services for public procurement	• Share of public administrations using the definition in their procurement activities (50%-100%) • Number of public administrations procuring cloud services • Time needed by public administrations to adopt the procedures • Time for public administrations to evaluate bids • Number of cloud and AI computing service providers that can participate in procurement processes aligning with the guidelines (244-350)	1.3 [-0.6 – 9.4]	PM12 shows high variability, as the outcome shifts from a small net cost in the min scenario to a very large net saving in the max one, which represents a considerable shift in magnitude and direction of impact. Therefore, the results of this measure depend heavily on the underlying assumptions. Results alternate between net costs and net benefits across scenarios, combined with large dispersion, implying low robustness and high sensitivity to modelling choices. The variability is driven by mainly two parameters. First, the average number of procured contracts every year for highly critical services in the EU public sector, spanning from 67 in the central and min values to 133. While the maximum value stems from the projections calculated considering the existing TED data multiplied by the estimated value of highly critical use case (5%, based on input from stakeholders), the interviews as part of the study led to the conclusion that a more conservative value for the central value was needed. Secondly, on the number of cloud providers that could participate in the bids. The study yielded the result that more than 400 cloud and AI computing service providers offer their services in the EU, while the estimates of providers that could comply with the

Policy Measure	Key Parameters varied	Central NPV and scenario range (€ m)[99]	Result and interpretation
			sovereignty criteria for their services range in the values of over 300.
PM15: Voluntary sovereignty risk assessments for the use of cloud and AI computing services in the public sector	• No. of FTEs required to get audited (10-20 FTEs) • No. of FTEs to maintain the audit (2-5 FTEs) • No. of MS that designate the competent authorities to carry out audit (5 - 27) • No. of MS that adopt and apply the voluntary sovereignty scheme, (5-27 MS)	316.8 [83.0 – 333.8]	PM15 generates high net savings in both scenarios, with outcomes improving greatly under the max assumptions..
PM16: Non-mandatory specific award criteria for the procurement of cloud and Ai computing services	• No. of public authorities procuring cloud and AI computing services • No. of tenders and offers per year • No. of cloud and AI computing service providers • Providers' effort to align to the award criteria	-17.1 [-4.9 – -28.3]	PM16 results in net costs in both min and max scenarios. While the PM generates some savings, these are not sufficient to outweigh costs. As above, this could be drive by the no. of estimated authorities procuring cloud and AI computing services and to the administrative effort needed by the providers to adapt to the new criteria.
PM17: Public Sector cloud federation	• Capacity shared by each MS with the federation (5%-15%) • No. of Member States participating in the federation • Energy efficiency (PUE, i.e. amount of data centre power dedicated to IT).	12 192.4 [7 878.4 – 16 506.4]	PM17 delivers high net cost savings across all scenarios. Given the difference between min-max scenarios, the PM looks sensitive to the underlying assumptions, e.g. MS participating in the federation or even capacity shared. This assumption-driven variability above 50% reduces precision, yielding medium–high confidence overall. As additional capacity is shared among MS, benefits increase substantially, as one could expect.
PM18: Vendor-neutral EU cloud/AI skill certificates	• No. of experts that can be certified on a yearly basis (100-500) • Certification fees ranging (EUR 50-150) • Effort saved by opting for a vendor-neutral certification, i.e. the number of certifications from other technologies and days saved • Coordination savings for the Commission from avoiding duplication of effort (EUR 0-21 067) • Reduced costs in the certification of similar technologies from different providers	74.3 [15.4 – 118.8]	PM18 generates net cost savings in both min and max scenarios, with benefits increasing significantly under the latter. The large dispersion (≥100%) reflects strong sensitivity to assumptions. Despite this, it consistently delivers a positive impact and becomes more efficient as cost savings scale.
PM19: Mandatory specific award criteria for the procurement of cloud and AI computing services	• No. of services audited on a yearly basis (NUTS 0:100- 500; NUTS 1: 50-150; NUTS 2: 50-150; NUTS 3: 20-30; min 220 services and max 830) • No. of hours saved due to automated dependency analysis per year (5 - 300 hours)	- 152.6 [-100.0 – - 213.0]	PM19 shows net costs across scenarios with medium-low variability.

Policy Measure	Key Parameters varied	Central NPV and scenario range (€ m)[99]	Result and interpretation
PM20: Boosting open source in public administrations	• No. of initial repositories that MS put in place (5 – 25) • Effort to maintain and govern repositories (0.6 - 1.2 FTE) • Costs to set up the OSPOs (EUR 2m-3m) • Costs to maintain the OSPOs (EUR 8m-28m) • Effort of OS projects developed in the public administrations (2-5 FTEs) • Contract values of OS projects developed for the public administrations (EUR 400 000-600 000) • Savings for not duplicating software, (EUR 80 000 – 450 000)	3 387.5 [478.9 – 9 172.5]	PM20 produces substantial net savings across all scenarios, making it one of the highest impact measures. Given the increase in savings from the min to the max scenario, the PM can be considered highly sensitive to the underlying assumptions. Indeed, extreme sensitivity to assumptions significantly weakens confidence in both magnitude and stability. Despite this large variation, it remains a robust measure generating net savings even under conservative assumptions.
PM21: Mandatory sovereignty risk assessments for the use of cloud and AI computing services in the public sector	• Effort to obtain the audit • No. of MS where CSPs would seek the audit/validation in the absence of a single market (5-27) • No. of cloud and AI computing services in possession of the audit • No of submitted bids per year.	1 343.6 [838.6 – 1699.4]	PM21 delivers consistent savings across all scenarios, with a modest level of sensitivity to the underlying assumptions. Assumption-driven uncertainty above 50% implies moderate confidence in scale.
PM22: EU-level procurement of cloud and AI computing services	• Time saved thanks to fewer coordination needs for national public authorities (0.1 - 0.5 FTEs) • FTEs saved thanks to joint procurement (0.1 - 0.5 FTEs) • Savings in terms of effort incurred by participating PAs due to the possibility to aggregate demand and compose services (0.1 - 0.5 FTEs) • Capacity shared by each MS with the federation (5% - 15%)	33 969.5 [18 940.9 – 48 998.2]	PM22 delivers large net cost savings across all scenarios. The increase from min to max indicates that the PM may be quite sensitive to the underlying assumptions. This large dispersion limits quantitative certainty. Despite this, it remains robust as even in the min scenario, cost savings are significant.
PM23: Financial support for SMEs to adopt cloud and AI	• Resources dedicated by SMEs for applications (10-30 working days)	-66.4 [-35.5 – -97.5]	PM23 presents net costs across all scenarios, although the overall scale is modest with respect to the other measures. Net costs stem also from the non-quantified strategic benefits generated by this measure. Assumption sensitivity introduces uncertainty (>50%) around central estimates.

Policy measures affecting permitting timelines and data centre deployment (PM4-PM5 and PM10) deliver substantial net savings/benefits in both minimum and maximum scenarios. Although the magnitude of savings is sensitive to adoption rates, months saved, deployment trajectories and PUE reductions, the impact of the measures remains positive even when such parameters change, demonstrating the efficiency of interventions that accelerate data centre project delivery. PM6-PM9 represent measures highlighting only costs for operators, national public authorities or the Commission as their benefits were either non-quantifiable or indirect. These measures exhibit low sensitivity overall, with modest variations across min-max scenarios and relatively small impacts with respect to the other measures. Results for PM11-

PM24 show a wide range of impacts. Most measures generate net savings under the different scenarios, even under conservative assumptions, thus demonstrating the robustness of results. At the same time, several PMs show high sensitivity to the underlying parameters. PM17, PM20, PM21 and PM22 stand out for their high impact and strong robustness, with large savings, while PM12 shows a mixed performance, shifting from net costs to net cost savings across the min and max scenarios. The variability of PM12 is driven by mainly two parameters. First, the average number of procured contracts every year for critical services in the EU public sector, spanning from 67 in the central and min values to 133. While the maximum value stems from the projections calculated considering the existing TED data multiplied by the estimated value of highly critical use case (5%, based on input from stakeholders), the interviews as part of the study led by Technopolis led to the conclusion that a more conservative value for the central value was needed. Secondly, on the number of cloud providers that could participate in the bids. The study led by Technopolis yielded the result that more than 400 cloud and AI computing service providers (see Annex 4) offer their services in the EU, while the estimates of providers that could comply with the sovereignty criteria for their services range in the values of over 300. These values were cross validated in the final validation workshop from the study led by Technopolis.

A sensitivity assessment was also performed for the measures evaluated using a discounted cash flow approach. While several variables influence project value, the analysis focused on those parameters that could be directly influenced by the policy intervention, i.e. 1) Power Usage Effectiveness (PUE), which affects operating costs and consequently the project's NPV and 2) Time savings, which impact the timing of revenues and discounting of future cash flows. In the model, reducing the project development timeline from 32 months to 26 months (6-month acceleration), increases NPV by around EUR 6.4 m, implying a sensitivity of around EUR 1.1 m of NPV per month of time saved. PUE affects operating costs by determining the electricity needed per unit of IT load. Reducing PUE levels while keeping the other assumptions unchanged, leads to around EUR 0.7 m of NPV for every 0.01 improvement in PUE.

While the model is sensitive to additional variables, these cannot be directly tackled by the class of policy measures under review. Utilisation and revenues are mostly influenced by market demand and commercial strategies. CAPEX levels are determined by construction market dynamics and technology costs, unless specific subsidies are applied. The WACC is predominantly affected by financial market conditions and sovereign risk, necessitating macro-financial instruments rather than operational regulations to influence it. Taxation and depreciation are dictated by national fiscal policies. Power prices are shaped by wholesale market rates and grid tariff structures. Therefore, the analysis concentrates on timeline and PUE, as both can be technically managed through targeted policies and hold significant economic importance.

This analysis will be particularly useful to better understand how to tailor future policy design. Given the available evidence and heterogeneity of measures evaluated, it has been instrumental to understand where the outcomes of each policy measure where more assumption-dependent or stable.

6. MULTI-CRITERIA DECISION ANALYSIS

The multi-criteria analysis has been carried out by Technopolis et al (2025) under the study "Study: cloud and AI". The models used, the criteria, weights of the impacts as well as the attained results are detailed next.

6.1. Models used for the multi-criteria analysis

The multi-criteria decision analysis (MCDA) has been implemented using three complementary models:

1) A simple additive model based on Multi-Attribute Utility Theory (MAUT)
2) Preference Ranking Organisation Method for Enrichment Evaluation (PROMETHEE II)
3) ELimination Et Choix Traduisant la REalité (ELECTRE III)

The use of multiple models allows to triangulate the results. Firstly, MAUT provides transparent aggregation, while PROMETHEE II and ELECRE III introduce preferences and outranking logics that test the robustness of the findings. The three methods provide three different categories of models: full compensatory (MAUT), partially compensatory (PROMETHEE II), and non-compensatory (ELECTREE III).

The three models are designed to work in combination:

1) MAUT provides a clear and transparent baseline;
2) PROMETHEE II is an outranking method and incorporates preference thresholds, capturing the strength of differences, allowing partial compensation;
3) ELCETREE III tests robustness and non-compensatory consistency, identifying cases where trade-offs between criteria are not acceptable. It also belongs to the outranking methods, but it incorporates preferences, indifferences and veto thresholds.

All models use the same normalised and weighted option-level dataset, enabling consistent interpretation across approaches.

6.1.1 Multi-Attribute Utility Theory (MAUT)

The MAUT approach[100] is a classical multi-criteria decision-making method based on utility theory. It uses utility functions to evaluate and compare alternatives based on multiple criteria. The process in MAUT typically involves the following approach:

1. Definition of the relevant criteria;
2. Assignation of weights to the criteria to reflect their relative importance;
3. Normalisation of the performance for each alternative; and
4. Computation of the utility function per policy option, as a weighted sum of its scores across all criteria, capturing the overall desirability of each option.

This approach makes it a fully compensatory model, meaning that a strong performance in one impact can offset weaker performance in another. The benefits of this model are simplicity and transparency. It provides a clear overall ranking of options while allowing the decomposition of results by impact area, making it easy to identify which dimensions drive performance differences.

In the current analysis, each policy option is assigned a normalised score for every sub-impact area based on the CATI surveys carried out with external stakeholders[101], and on the estimated

[100] Jansen, S.J.T. (2011). The Multi-attribute Utility Method. In: Jansen, S., Coolen, H., Goetgeluk, R. (eds) The Measurement and Analysis of Housing Preference and Choice. Springer, Dordrecht. https://doi.org/10.1007/978-90-481-8894-9_5

[101] The CATI survey gathered feedback from key stakeholder groups, including public authorities, data centre operators, cloud and AI service providers, industry associations, and domain experts. Respondents were asked to assess the expected effectiveness and impact of a series of policy measures addressing two main problems: limited availability of sustainable

data on costs and savings presented in the sections above. These are multiplied by their respective impact and sub-impact weights. The resulting composite scores provide a straightforward and replicable measure of performance across scenarios.

The MAUT model employs an **additive aggregation structure**, assuming preferential independence across criteria. Each policy option $A_i$receives a utility score calculated as:

$$U(A_i) = \sum_{k=1}^{n} w_k \cdot u_k(A_i)$$

where:

1) $u_k(A_i)$is the normalised score for impact $k$under option A_i;
2) $w_k$is the composite weight derived from the impact and sub-impact levels.

The MAUT additive model serves as the foundation for comparison with the more preference-based methods (PROMETHEE II and ELECTRE III), as described next.

6.1.2 Preference Ranking Organisation Method for Enrichment Evaluation (Promethee II)

The Preference Ranking Organisation Method for Enrichment Evaluation (PROMETHEE II)[102] is a preference-based and partially compensatory method. It differs from the additive models by considering how strongly one policy option is preferred over another on each criterion, rather than aggregating scores directly. PROMETHEE II compares every pair of alternatives across all criteria and calculates a preference degree that expresses the extent to which one option performs better than another. These degrees are then combined into positive and negative preference flows to establish a final net ranking of the option. A positive flow represents how much the option outranks the other while a negative one shows how much it is outranked. The net flow (positive minus negative) provides a full ranking of the alternatives. This approach is valuable because it incorporates thresholds to reflect realistic decision-making behaviour, recognising that small performance differences may be insignificant while larger one signal a clear preference.

Thresholds

For each criterion k, two thresholds are defined:

1) an *indifference threshold* (q), below which the difference between two options is negligible. This was set to 0.25 of the total score range.
2) a *preference threshold* (p), beyond which one option is clearly preferred. This was set to 0.50 of the total score range.

---

computing capacity infrastructure in the EU, and limited availability of European cloud services including for highly critical use cases. Each measure was rated on a likert seven-point scale from strong decrease to strong increase, complemented by ranking exercises to identify the most effective packages and instruments. 119 stakeholders (114 economic operators and 5 Public Authorities) assessed expected changes in impact areas under each policy measure using a seven-point scale (from strong decrease = -3 to strong increase = +3).

[102] J. Figueira, S. Greco, M. Ehrgott. Multiple Criteria Decision Analysis State of the Art Surveys. Springer, Berlin (2005). 1045 pp

By using these thresholds, the model allowed limited compensation and avoided over-ranking options that performed only marginally better on criteria. PROMETHEE II is therefore effective for policy evaluations involving mixed quantitative and qualitative evidence, as it can reflect nuanced stakeholder preferences while still providing a complete ranking of options.

PROMETHEE II is a **preference-based, partially compensatory** method relying on pairwise comparisons between alternatives. For each pair (A_i, A_j), the method computes a preference degree $\pi_{ij}^k \in [0,1]$for each criterion k, based on the difference in their performance:

$$\pi_{ij}^k = f_k(d_{ij}^k)$$

where $d_{ij}^k = u_k(A_i) - u_k(A_j)$and $f_k$is a preference function defined by:

1) *Indifference threshold* q_k: differences below this are considered negligible;
2) *Preference threshold* p_k: differences above this imply strict preference.

The overall preference index between $A_i$and $A_j$is:

$$\Pi_{ij} = \sum_{k=1}^{n} w_k \pi_{ij}^k$$

Positive (ϕ^+) and negative (ϕ^-) flows are then computed:

$$\phi^+(A_i) = \frac{1}{m-1}\sum_{j\neq i} \Pi_{ij}, \phi^-(A_i) = \frac{1}{m-1}\sum_{j\neq i} \Pi_{ji}$$

The **net flow** ($\phi(A_i) = \phi^+ - \phi^-$) provides a complete ranking of the alternatives.

6.1.3 ELimination Et Choix Traduisant la REalité (Electre III)

The ELimination Et Choix Traduisant la REalité (ELECTRE III)[103] method is an outranking approach. Unlike MAUT, or PROMETHEE II, it does not assume that trade-offs between criteria are always acceptable. Instead, it tests whether there is sufficient evidence to state that one policy option outranks another, i.e. performs at least as well overall, without being significantly worse on any major criterion.

ELECTRE III is a non-compensatory model, which makes it useful when some criteria (e.g. environmental sustainability) are considered essential and should not be fully offset by gains elsewhere. It combines two types of information:

1) *Indifference threshold* (q): small differences are ignored. This was set to 0.25 of the total score range.
2) *Preference threshold* (p): a preference threshold (p), larger differences indicate a clear preference. This was set to 0.50 of the total score range.

[103] Uzun, B., Bwiza, R.A., Uzun Ozsahin, D. (2021). ELimination Et Choix Traduisant La REalité (ELECTRE). In: Uzun Ozsahin, D., Gökçekuş, H., Uzun, B., LaMoreaux, J. (eds) Application of Multi-Criteria Decision Analysis in Environmental and Civil Engineering. Professional Practice in Earth Sciences. Springer, Cham. https://doi.org/10.1007/978-3-030-64765-0_5

3) *Veto threshold* (v): if the difference exceeds this level, one criterion can block the overall outranking regardless of others.

Thresholds are set to match chosen the way the PROMETHEE model is configured. ELECTRE III is particularly beneficial in regulatory and policy contexts, as it can identify incomparability i.e. cases where neither option is clearly superior, which mirrors complexity of multi decision-making.

Summarizing, ELECTRE III is a **non-compensatory outranking** method that assesses whether one alternative "outranks" another by combining *concordance* (agreement) and *discordance* (veto) indices.

For each pair of alternatives (A_i, A_j):

1) A *concordance index* C_{ij}expresses the degree to which criteria support the statement "A_i is at least as good as A_j":

$$C_{ij} = \sum_{k \in K} w_k \, c_k(A_i, A_j)$$

where $c_k$is the partial concordance per criterion.

2) A *discordance index* D_{ij}measures the extent of opposition to that statement, identifying criteria where $A_j$substantially outperforms A_i.
3) A *credibility index* $S_{ij}$is then computed as:

$$S_{ij} = C_{ij} \times \prod_{k \in \text{discordant}} \frac{1 - D_{ij}^k}{1 - C_{ij}}$$

which quantifies the overall strength of the outranking relation.

The final ranking is obtained through exploitation procedures, balancing credibility thresholds and identifying dominance, indifference, and incomparability relations

6.1.4 Summary of models used for the multi-criteria analysis

The table below depicts a summary of the models used for this MCDA with their main characteristics.

Table 46. Summary of models used for the multi-criteria analysis

Feature	MAUT	PROMETHEE II	ELECTRE III
Method type	Compensatory, utility-based aggregation	Outranking with pairwise preference flows	Outranking with credibility and discordance indices
Compensation	Fully compensatory	Semi-compensatory	Non-compensatory (veto can block dominance)
Output	Full ranking	Full ranking	Partial ranking
Thresholds	None	Uses preference functions	Uses explicit indifference, preference and veto thresholds

Feature	MAUT	PROMETHEE II	ELECTRE III
Strengths	Easy and clear to communicate	Pairwise comparisons	Handles uncertainty, and incorporates veto
Data used	Quantitative scores and weights	Quantitative, but requires selecting preference functions	Mixed data, requires defining discordance and credibility indices

6.2. Development and comparisons of policy options (MCDA)

The multi-criteria decision analysis allows to evaluate the relative performance of different policy options under study. It enables a systematic comparison of alternatives when multiple and often conflicting objectives must be considered.

The analysis combined quantitative data from two sources:

1) *Survey data,* in which 119 stakeholders (114 economic operators and 5 Public Authorities) assessed expected changes in impact areas under each policy measure using a seven-point scale (from strong decrease = -3 to strong increase = +3). The sample is described below.
2) *Estimated data* developed through quantitative modelling, covering administrative costs, adjustment costs, and cost-saving for each policy measure.

All data is first combined and harmonised to create a single dataset covering all policy options, policy measures, impact areas, and sub-impact areas.

Weights are applied to reflect the relative importance of each impact and sub-impact. The reference case is equal weighting. Given the different nature that the two problems deal with, different weights for problem 1 and problem 2 are also considered.

The impact-level weights define the overall direction of the assessment by indicating which broad dimensions carry the greatest influence under each scenario. In the equal weighting scenario, all four impacts – economic/effectiveness, costs/efficiency, social and environmental - are weighted equally (25%). Under Problem 1 (P1), the weighting shifts towards the economic/effectiveness dimension (40%), highlighting the priority of accelerating deployment and enhancing efficiency, while social impacts receive reduced emphasis (5%). For Problem 2 (P2), the weighting moves towards costs and economic/effectiveness (55%) impacts, reflecting a focus on sovereignty, trust, and resilience.

Table 47. Impacts weighting (Source: Technopolis et al. (2025))

Impact	Equal weighting [EW]	P1 weights	P2 weights
Economic/effectiveness	25%	40%	55%
Costs/efficiency	25%	35%	35%
Social	25%	5%	5%
Environmental	25%	20%	5%

The sub-impact weights specify how the detailed components within each impact contribute to the overall evaluation. Under the equal weighting scenario, the weights are balanced across sub-criteria. Under Problem 1, the emphasis shifts towards sub-impacts linked to rapid deployment, computing capacity, and cost efficiency, aligning with the scenario’s objective of speeding up infrastructure expansion. Conversely, Problem 2 introduces a strong emphasis on digital sovereignty, open source capacity, customer choice, and transparency, consistent with its social and governance orientation. Environmental sub-impacts source also adjust, prioritising reductions in data centre footprints under Problem 1 and digital sovereignty, and resilience under Problem 2.

Table 48. Sub-impacts weighting (Source: Technopolis et al. (2025))

Sub-Impact	Equal weighting sub - impact	P1 weights sub - impact	P2 weights sub - impact
Speed of construction and deployment of data centres	14%	30%	0.5%
Computing capacity for AI services and general purpose computing	14%	20%	0.5%
Adoption of high-performance, low-carbon, energy-efficient cloud and AI computing services	14%	25%	0.5%
Cross-border market access for EU-based cloud and AI computing service providers	14%	10%	14.5%
Digital sovereignty and resilience in the public sector including through public procurement	14%	7%	50%
Open source capacity	14%	5%	14.5%
Ensuring customer choice and the ability to switch providers across layers of the AI compute stack	14%	3%	19.5%
Administrative costs	25%	15%	15%
Adjustment costs	25%	15%	15%
cost savings	25%	30%	30%
net costs	25%	40%	40%
Transparency and citizen trust	50%	60%	65%
Citizen/community engagement	50%	40%	35%
Data centres environmental footprint (energy, water use, greenhouse gas emissions)	50%	70%	50%
Leveraged investments from public and private actors for sustainable infrastructure and services	50%	30%	50%

In this framework, the sub-impact weights shown in the table below are derived from the product of the higher-level impact weights and the relative importance of each sub-impact within that impact area.

The calculation works in two steps:

1. Each main impact area, Economic/effectiveness, Costs/efficiency, Social, and Environmental, is first assigned an overall weight at the impact level (for example, under Problem 2: Economic/effectiveness = 55%, Costs = 35%, Social = 5%, Environmental = 5%).
2. Within each impact area, that total weight is distributed across its constituent sub-impacts according to their relative importance in the scenario. The weight of each sub-

impact is therefore the impact-level weight multiplied by its share within that impact group.

For instance, under Problem 2, the Economic/effectiveness impact (55%) is subdivided across seven sub-impacts, with digital sovereignty and resilience receiving a larger internal share than speed of construction. Multiplying this impact weight (55%) by the internal share of digital sovereignty and resilience (around 35%) yields a sub-impact weight of roughly 12.3% in the table. The same process applies across all impact areas: the economic/effectiveness weight (55%) multiplied by the internal weighting for digital sovereignty and resilience in the public sector including through public procurement (50%) produces a final sub-impact weight of 27.5%.

This hierarchical weighting ensures that the total of all sub-impacts adds up to 100% and that each sub-impact's influence on the final composite score reflects both:

1. The relative priority of its parent impact area (e.g. Social vs Effectiveness/economic), and
2. The specific emphasis placed on that sub-impact within the impact group (e.g. within Social, transparency outweighs engagement).

Table 49. Sub-impacts weighting used (Source: Technopolis et al. (2025))

Sub-Impact	Equal weighting sub - impact	P1 weights sub - impact	P2 weights sub - impact
Speed of construction and deployment of data centres	3.57%	12.0%	0.3%
Computing capacity for AI services and general purpose computing	3.57%	8.0%	0.3%
Adoption of high-performance, low-carbon, energy-efficient cloud and AI computing services	3.57%	10.0%	0.3%
Cross-border market access for EU-based cloud and AI computing service providers	3.57%	4.0%	8.0%
Digital sovereignty and resilience in the public sector including through public procurement	3.57%	2.8%	27.5%
Open source capacity	3.57%	2.0%	8.0%
Ensuring customer choice and the ability to switch providers across layers of the AI compute stack	3.57%	1.2%	10.7%
Administrative costs	6.25%	5.3%	5.3%
Adjustment costs	6.25%	5.3%	5.3%
cost savings	6.25%	10.5%	10.5%
net costs	6.25%	14.0%	14.0%
Transparency and citizen trust	12.50%	3.0%	3.3%
Citizen/community engagement	12.50%	2.0%	1.8%
Data centres environmental footprint (energy, water use, greenhouse gas emissions)	12.50%	14.0%	2.5%

Sub-Impact	Equal weighting sub - impact	P1 weights sub - impact	P2 weights sub - impact
Leveraged investments from public and private actors for sustainable infrastructure and services	12.50%	6.0%	2.5%

6.2.1 Summary of results multi-criteria decision analysis

In both Problem 1 and Problem 2, all policy options perform better than the baseline, consistently across the three methods tested and stakeholder groups (AI and cloud service providers, data centre operators, National Public Authorities and SMEs). The assessment therefore confirms that maintaining the status quo is the least attractive option, and that intervention is warranted from both an effectiveness and efficiency perspective.

The multi-criteria analysis is based on the original specification of policy options. While some measures were subsequently refined, the options were retained in their initial form to ensure comparability across scenarios. The results draw on stakeholder survey data collected in August-September 2025 and cost inputs updated in early 2026. As such the findings should be interpreted as indicative, reflective the relative performance of the options.

The table below presents an overview of the comparative performance of the options across methods and weighting schemes.

Table 50. Summary of option performance across methods and problems (Source: Technopolis et al. (2025))

Problem	Method	Main conclusion
P1	MAUT	PO1-B and PO1-C are strongest, especially under P1 weights.
P1	PROMETHEE II	PO1-B and PO1-C clearly ahead; PO1-A only modest improvement.
P1	ELECTRE III	Ranking: PO1-B > PO1-C > PO1-A = baseline
P2	MAUT	Under P2 weights, PO2-B and PO2-C are strongest
P2	PROMETHEE II	PO2-C best, PO2-A second; PO2-B weak, close to baseline under P2 weights
P2	ELECTRE III	PO2-C clearly first; PO2-A and PO2-B at best marginal over baseline

Problem 1

For Problem 1, all three options (PO1-A/B/C) deliver a clear improvement over the baseline in all three methods, namely, MAUT, PROMETHEE II and ELECTRE III. Under equal weighting, MAUT shows that all options achieve positive total scores, while the baseline remains negative. When Problem 1 weights are applied the differences between options become more pronounced. In this configuration, PO1-B and PO1-C clearly outperform PO1-A, and the baseline remains the weakest.

Across the three methods, a consistent pattern emerges:

- PO1-B (legislative and financial intervention enforced nationally) and PO1-C (legislative and financial intervention enforced at EU-level) are the strongest options and both strongly dominate the baseline.
- PO1-A (collaborative framework) provides only a moderate improvement over the baseline: positive overall, but not comparable in magnitude to the more interventionist options.

The baseline never outranks any option and is always clearly dominated in the outranking analyses.

At **measure level**:

- For PO1-A, PM3 (guidelines on sustainable data centres) is the main driver of performance, as it is the only measure that clearly turns the cost score positive under Problem 1 weights and contributes solidly to the total score. PM1 (Alliance working group) and PM2 (stakeholder forum) add small but consistent gains on effectiveness and social criteria but remain modest.
- Within PO1-B, performance is driven by PM4 (project facilitator for the roll-out of data centres) and PM5 (fast-track area identification). These measures combine improved cost outcomes with strong effectiveness and therefore explain the option's high overall score.
- In PO1-C, all measures contribute positively, but PM10 (EU-level identification of fast-track areas) stands out, especially under Problem 1 weights, by delivering the best cost outcome in the package alongside strong effectiveness. PM8 (EU R&D funding) and PM9 (EU deployment funding) generate clear environmental and social benefits with a high effectiveness but retain slightly negative cost scores, reflecting the associated cost burdens.

Stakeholder-specific results show that all groups are better off than in the baseline for all options, but they differ in their preferred bundle:

- Economic operators favour PO1-B, with PO1-C close behind, driven by better cost and effectiveness outcomes.
- National public authorities also obtain the highest scores under PO1-B, followed by PO1-C; PO1-A is positive but less attractive. Improvements for authorities arise mainly from better cost outcomes relative to the baseline and small social and environmental gains, rather than from direct effectiveness.
- CSPs and AI service providers see substantial improvements under all options but show a clear preference for PO1-B, particularly when Problem 1 weights are applied, reflecting the importance of streamlined permitting and deployment-oriented measures.
- SMEs benefit substantially from all options relative to the baseline, but PO1-B is the most favourable bundle, as it combines improved costs with higher effectiveness and social scores for this group.

The evidence for Problem 1 suggests that PO1-B is the most attractive option when priority is given to deployment and cost efficiency, while PO1-C is favoured when it comes to social and environmental benefits, at the expense of somewhat higher perceived cost intensity in EU-level funding measures. PO1-A offers a modest, low-intensity improvement but does not match the performance of the more ambitious packages.

Problem 2

For Problem 2, all three options (PO2-A/BC) perform clearly better than the baseline across the three MCDA methods. Under equal weighting in MAUT, total scores for all options indicate broad improvements in effectiveness, social and environmental outcomes. When Problem-2 weights are applied all options improve further and remain clearly above the baseline, with PO2-B and PO2-C achieving the highest MAUT scores.

However, once outranking approaches are considered, a stable pattern emerges:

- PO2-C (EU-coordinated procurement and framework) is the strongest option overall. Both PROMETHEE II and ELECTRE III identify PO2-C as the preferred option, under both equal and Problem-2 weights.

- PO2-A (transparency and visibility) is consistently a secondary but clearly positive option, always better than the baseline but not reaching the performance of PO2-C.
- PO2-B (voluntary EU framework) is, at best, marginally better than the baseline in ELECTRE III and is clearly weaker than PO2-C (and often PO2-A) in PROMETHEE II, particularly when Problem-2 weights are applied.

At **measure** level:

- For PO2-A, the strongest contributors are PM11 (creating a sovereign cloud and AI computing services definition), PM12 (guidelines for sovereign services) and PM14 (interoperability flanking measures). These measures are seen as useful and relatively low-cost, particularly once sovereignty and resilience gain more weight. PM13 (annual sovereignty conference) provides only limited added value and mainly adds some cost, resulting in lower total scores.
- In PO2-B, performance is driven by PM15 (sovereignty scheme) and PM17 (cloud federation), which combine neutral or positive cost impacts with solid effectiveness and social gains. PM18 (training programme) generates moderate, clearly positive contributions, while PM16 (voluntary award criteria) is weaker.
- Within PO2-C, PM20 (promotion of open source use) and PM22 (EU-level procurement and federation) are the main drivers of performance, combining manageable or slightly positive cost effects with strong effectiveness and social benefits when sovereignty-related dimensions are prioritised. PM21 (mandatory use of audited services and award criteria) becomes more attractive under Problem-2 weights, while PM23 (SME support) has low totals and negative cost scores, limiting its contribution to the option's overall strength.

Stakeholder-specific results for Problem 2 again indicate clear improvements relative to the baseline for all groups, but with notable differences in preferences:

- Economic operators see all options as an improvement, but clearly prefer PO2-C, which combines the strongest cost outcome with robust effectiveness and social gains. PO2-A is generally second, with PO2-B weaker overall.
- National Public Authorities favour PO2-B under EW and PO2-C under P1 weights. PO2-A remains positive but leaves a more significant cost burden; PO2-C offers smaller gains and only marginal cost improvements from their perspective versus PO2-B also under P2 weights.
- Cloud and AI computing service providers see substantial gains under all options, but PO2-C is the preferred grouping, particularly when Problem-2 weights are applied, with PO2-A second in EW and PO2-B only marginally improving over PO2-A under P2 weights.
- SMEs benefit substantially from all options compared to the baseline, but PO2-A is the most favourable option under EW and PO1-C is the preferred one under P1 weights, as it combines the least negative cost scores with the highest economic and social benefits for this group.

The results for Problem 2 indicate that PO2-C is the most robust option at system level, especially when non-compensatory trade-offs and sovereignty-focused priorities are considered, while PO2-B is most attractive for national public authorities and PO2-A is particularly beneficial for SMEs. All three options remain markedly superior to the baseline, confirming that a policy response to Problem 2 is justified.

6.2.2 Multi-criteria analysis for Problem 1

MAUT results for Problem 1 show a clear improvement of all three policy options (PO1-A/B/C) over the baseline across both weighting schemes. Under equal weighting, all options deliver positive total scores (0.399 for PO1-A, 0.575 for PO1-B, 0.513 for PO1-C), while the baseline is distinctly negative (-0.359). This reflects the fact that the measures jointly improve effectiveness, environmental and social outcomes relative to the status quo, while also reducing the net cost burden. Social impacts are consistently positive for all options and negative for the baseline, and environmental impacts also improve slightly relative to the baseline under equal weighting.

When shifting to the Problem 1 weighting (which places more emphasis on effectiveness and cost impacts, and sustainability), the overall ranking is broadly stable but the differences between options become more pronounced. PO1-B and PO1-C clearly dominate, with total scores of 0.688 and 0.545 respectively, compared to 0.312 for PO1-A and -0.387 for the baseline. The reweighting particularly favours PO1-B, which combines the strongest performance in terms of effectiveness with the best cost-benefit outcome (costs turning positive under P1), while still performing better than the baseline on environmental and social dimensions. This suggests that, under a deployment-focused policy perspective, PO1-B (and to a slightly lesser extent PO1-C) represent the most attractive bundle of measures among the options considered.

Table 51. MCDA Aggregate Results MAUT – Problem 1 (Source: Technopolis et al. (2025))

	Costs/efficiency		**Effectiveness**		**Environmental**		**Social**		**Total**	
Option	EW	P1	EW	P1	EW	P1	EW	P1	EW	P1
Baseline	-0.538	-0.714	0.242	0.470	-0.037	-0.134	-0.026	-0.008	-0.359	-0.387
PO1-A	-0.119	-0.128	0.246	0.421	0.055	-0.024	0.216	0.043	0.399	0.312
PO1-B	-0.011	0.143	0.298	0.543	0.074	-0.041	0.214	0.043	0.575	0.688
PO1-C	-0.089	0.017	0.307	0.520	0.078	-0.036	0.216	0.044	0.513	0.545

The PROMETHEE II results for Problem 1 clearly indicate that PO1-B and PO1-C are the strongest options, with PO1-B emerging as the preferred options once Problem 1 priorities are reflected. Under equal weighting, most options improve on the baseline which shows strongly negative net flows at both impact and sub-impact level (–0.917 and –0.798). At impact level, PO1-B strongly outperforms PO1-C with positive impact-level flows (0.500 vs 0.189), while PO1-A delivers only a modest gain with respect to the baseline (-0.189). At the sub-impact level, PO1-B still outperforms PO1-C but the difference between the two options decreases (0.312 vs 0.289), suggesting a marginal advantage when all criteria are treated as equally important.

When the Problem 1 weighting is applied, the ordering becomes more pronounced. The baseline remains negative (–0.867 at impacts; –0.671 at sub-impacts), and PO1-A remains negative at both levels (–0.447 impacts; –0.331 sub-impacts), indicating limited alignment of this option with deployment- and cost-driven priorities. By contrast, PO1-B and PO1-C both achieve high impact-level flows (0.583 and 0.147). At the sub-impact level under P1, PO1-B (0.413) outperforms PO1-C (0.252), which points to PO1-B as the best overall option once implementation-level effects and the stronger emphasis on effectiveness and cost criteria are considered.

Table 53. PROMETHEE II - Problem 1 (Source: Technopolis et al. (2025))

Option	**EW - Impacts**	**EW Sub-impacts**	**P1 - Impacts**	**P1 – Sub-Impacts**
Baseline	-0.917	-0.798	-0.867	-0.671
PO1-A	-0.189	-0.112	-0.447	-0.331
PO1-B	0.500	0.312	0.583	0.413
PO1-C	0.189	0.289	0.147	0.252

For Problem 1, the ELECTRE III outranking analysis shows a very consistent pattern: at impact level, both under equal weighting and under the P1 weights, the descending order is PO1-B > PO1-C > PO1-A = baseline, meaning that PO1-B outranks PO1-C, and both outrank the baseline, while PO1-A does not. At the sub-impact level, in both EW and P1 options the ranking changes making PO1-C > PO1-B > baseline = PO1-A, with high credibility indices for the outranking relations between PO1-C and the other options. In other words, once non-compensatory trade-offs and detailed criteria are fully taken into account, PO1-C is the strongest option, closely followed by PO1-B, while PO1-A is barely better than or equal to the baseline and never outranks the two more ambitious options. The difference in these results between the impact level and the sub-impact results reflects how the structure of the analysis influences the comparison of the options. When impacts are assessed at a broader level, strong performance in one area can offset weaker performance in another, i.e. making PO1-B appear preferrable. However, when this analysis is performed at sub-impact level, the trade-offs are no longer absorbed within the broader categories, i.e. PO1-C performs more evenly and therefore emerges as the strongest option. The different ranking thus reflects the differences in how balanced the policy options are. PO1-B appears to generate higher overall impacts but with greater divergence across cost-benefit, effectiveness, environmental and social dimensions, whereas PO1-C delivers more balanced, though less pronounced results across these criteria. Importantly, PO1-B and PO1-C both outperform PO1-A which does not improve over the baseline and thus represent improvements over the status quo.

Table 54. ELECTRE III ranking of options – Problem 1 (Source: Technopolis et al. (2025))

Option	Impact level (EW)	Sub-impact level (EW)	Impact level (P1)	Sub-impact level (P1)	Overall judgement
PO1-B	1	2	1	2	Very strong
PO1-C	2	1	2	1	Very strong
PO1-A	3 = Baseline	3 = Baseline	3 = Baseline	3 = Baseline	Weak improvement over baseline
Baseline	3 = PO1-A	3 = PO1-A	3 = PO1-A	3 = PO1-A	Reference

Stakeholder analysis

For economic operators, all three options represent a marked improvement over the baseline, but with a clear hierarchy. Under both equal weighting and the Problem 1 weighting, PO1-B performs best overall (0.623 and 0.742), closely followed by PO1-C, with PO1-A some distance behind. The main driver is the combination of improved cost outcomes and stronger effectiveness scores: PO1-B is the only option that yields clearly positive cost results for operators under EW (0.045), while also outranking the other options under P1 weights in terms of costs. PO1-B delivers the highest effectiveness score (0.538) under P1 weighing while PO1-C outperforms it under EW. Environmental scores for operators improve modestly under equal weighting but turn slightly negative under P1 (reflecting the lower weight and some trade-offs), whereas social scores are clearly higher than the baseline for all options. The data suggest that economic operators have better results with national simplification and fast-track mechanisms (PO1-B) as they are offering the best balance of lower burdens and stronger business opportunities, with EU-level interventions (PO1-C) being also attractive but slightly less beneficial in net terms.

For national public authorities, all options also outperform the baseline, but preference patterns differ and the gains are more modest. Under equal weighting, PO1-B slightly dominates (0.281

vs 0.259 for PO1-C and 0.050 for PO1-A), driven by the strongest combination of cost, social and environmental scores. Under the Problem 1 weighting, PO1-B still has the highest total score (0.408), but PO1-C moves farther (0.185), while PO1-A remains the weakest performer, albeit still clearly above the baseline. A notable contrast with operators is that the effectiveness dimension for public authorities is closer to, or slightly below, the baseline, especially under P1, suggesting that administrations anticipate less direct effectiveness from the measures. Instead, their improvement comes mainly from better cost outcomes relative to the baseline (particularly under PO1-B) and small but positive social and environmental effects. In sum, authorities tend to favour the national level option (PO1-B), which offers a better overall balance of impacts from their perspective, even if PO1-C performs best in terms of environmental impact (under EW) and social impacts, mostly in relation to the measures focused on funding for strategic and energy-efficient projects.

Table 55. MCDA Economic Operators and Public Authorities MAUT – Problem 1 (Source: Technopolis et al. (2025))

Impact	Costs		Effectiveness		Environmental		Social		Total	
	Economic Operators									
Option	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**
Baseline	-0.529	-0.703	0.260	0.504	-0.038	-0.141	-0.003	-0.004	-0.309	-0.344
PO1-A	-0.137	-0.156	0.238	0.410	0.040	-0.036	0.203	0.041	0.344	0.259
PO1-B	0.045	0.216	0.298	0.538	0.058	-0.058	0.223	0.045	0.623	0.742
PO1-C	-0.063	0.049	0.313	0.527	0.059	-0.057	0.229	0.046	0.538	0.564
	National Public Authorities									
Option	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**
Baseline	-0.390	-0.478	0.143	0.374	-0.125	-0.160	0.000	0.003	-0.373	-0.262
PO1-A	-0.064	-0.055	0.063	0.096	-0.010	-0.038	0.063	0.013	0.050	0.015
PO1-B	-0.023	0.108	0.188	0.333	0.004	-0.056	0.113	0.023	0.281	0.408
PO1-C	-0.097	-0.101	0.195	0.304	0.021	-0.047	0.141	0.028	0.259	0.185

For cloud and AI computing service providers, all three options improve on the baseline when impacts are equally weighted, with total scores rising from 0.267 (baseline) to 0.440 (PO1-A), 0.542 (PO1-B) and 0.572 (PO1-C). Since cost impacts are neutral under this Problem (all zero), the gains come from stronger effectiveness and social performance, with modest environmental improvements under equal weighting. Under the Problem 1 weighting, which amplifies effectiveness dimensions, the picture is more nuanced: PO1-A is essentially indistinguishable from the baseline (0.378 vs 0.381), while PO1-B and PO1-C provide clear net benefits (0.499 and 0.488 respectively), driven by higher effectiveness scores. Environmental scores for providers become slightly more negative under P1, indicating perceived trade-offs as deployment objectives are prioritised, but these are more than offset by the effectiveness and social gains in PO1-B and PO1-C.

For data centre operators, the options deliver very substantial improvements over the baseline across both weighting schemes. Under equal weighting, the total score rises from –0.501 (baseline) to 0.505 (PO1-A), 0.767 (PO1-B) and 0.654 (PO1-C), with a similar pattern under P1 (–0.438 to 0.399, 0.848 and 0.670 respectively). The baseline is characterised by strongly negative cost scores and only modest effectiveness, whereas PO1-B in particular moves higher (0.767 EW, 0.848 P1) while also delivering the highest effectiveness and social scores. PO1-A and PO1-C also perform very well, but their cost outcomes are weaker than PO1-B's. Environmental performance improves markedly relative to the baseline under equal weighting (especially in PO1-C), though again becomes slightly negative under P1 as the model places more emphasis on economic deployment. Overall, operators clearly favour the more interventionist national package in PO1-B, with PO1-C and PO1-A still representing substantial improvements over the status quo.

For SMEs[104], results show that all three options perform substantially better than the baseline, with PO1-C as the most favourable option under EW and PO1-B under P1 weights. All options improve over the baseline levels, yielding positive totals of 0.444 (PO1-A), 0.612 (PO1-B) and 0.629 (PO1-C) under EW. The improvement is driven by higher effectiveness scores (up to 0.320 for PO1-C) and clearly positive social and environmental contributions. When the Problem 1 weighting is applied, the ordering changes: PO1-B performs best (total 0.561), followed by PO1-C (0.526) and PO1-A (0.391), showing that as economic deployment is emphasized over other criteria, SMEs tend to favour PO1-B rather than an EU-level approach. Indeed, under P1, PO1-B improves mainly driver by higher effectiveness (0.569) compared to the other options and the baseline.

Table 56. MCDA Cloud and AI Computing Service Providers and Data Centre Operators MAUT – Problem 1 (Source: Technopolis et al. (2025))

Impact	Costs		Effectiveness		Environmental		Social		Total	
Cloud and AI Computing Service Providers										
Option	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**
Baseline	0.000	0.000	0.262	0.508	-0.026	-0.129	0.031	0.002	0.267	0.381
PO1-A	0.000	0.000	0.223	0.386	0.028	-0.046	0.189	0.038	0.440	0.378
PO1-B	0.000	0.000	0.286	0.520	0.050	-0.062	0.205	0.041	0.542	0.499
PO1-C	0.000	0.000	0.306	0.514	0.046	-0.070	0.220	0.044	0.572	0.488
Data Centre Operators										
Option	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**
Baseline	-0.534	-0.711	0.253	0.492	-0.083	-0.191	-0.137	-0.029	-0.501	-0.438
PO1-A	-0.142	-0.164	0.298	0.509	0.089	0.002	0.260	0.052	0.505	0.399
PO1-B	0.046	0.219	0.342	0.609	0.087	-0.039	0.292	0.059	0.767	0.848
PO1-C	-0.063	0.048	0.340	0.576	0.109	-0.008	0.269	0.054	0.654	0.670
SMEs										
Option	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**	**EW**	**P1**
Baseline	0.000	0.000	0.233	0.453	-0.039	-0.132	-0.028	-0.011	0.166	0.311
PO1-A	0.000	0.000	0.222	0.386	0.039	-0.032	0.182	0.036	0.444	0.391
PO1-B	0.000	0.000	0.314	0.569	0.062	-0.056	0.237	0.047	0.612	0.561
PO1-C	0.000	0.000	0.320	0.529	0.061	-0.053	0.248	0.050	0.629	0.526

6.2.3 Multi-criteria analysis for Problem 2

For Problem 2, all three options outperform the baseline clearly under both equal weighting and the Problem 2 weighting, but with a distinct ordering. Under equal weighting, total scores move from a negative baseline (-0.183) to moderately positive values for all options (0.439 for PO2-A, 0.418 for PO2-B, 0.488 for PO2-C), reflecting broad improvements across effectiveness, social and environmental dimensions despite remaining negative on costs. When the Problem 2 weighting is applied, placing greater emphasis on economic and sovereignty-related aspects, overall performance improves substantially and differences between options

[104] SMEs account for cloud and AI computing service providers. Data centers are not included.

become more marked. The baseline remains negative (-0.220), while PO2-A rises to 0.572 and PO2-B and PO2-C reach 0.709 and 0.928 respectively.

The shift to the P2 weighting particularly benefits PO2-B and PO2-C because they combine improved cost outcomes (costs turn positive under P2 for both) with strong gains on the effectiveness dimension, which carries the highest weight in this scenario. Social scores are consistently positive and higher than the baseline for all three options in both weighting schemes, and environmental scores, while modest, also improve relative to the status quo. PO2-A and PO2-B perform well but are clearly dominated PO2-C under P2, indicating that more ambitious and coordinated intervention on sovereignty and uptake delivers a better balance of costs and benefits when judged against the Problem 2 policy priorities.

Table 57. MCDA Results MAUT – Problem 2 (Source: Technopolis et al. (2025))

	Costs/efficiency		**Effectiveness**		**Environmental**		**Social**		**Total**	
Option	EW	P1	EW	P1	EW	P1	EW	P1	EW	P1
Baseline	-0.361	-0.547	0.242	0.345	-0.037	-0.007	-0.026	-0.010	-0.183	-0.220
PO2-A	-0.098	-0.103	0.241	0.614	0.048	0.010	0.249	0.051	0.439	0.572
PO2-B	-0.009	0.168	0.228	0.490	0.046	0.009	0.199	0.041	0.418	0.709
PO2-C	-0.027	0.257	0.192	0.612	0.056	0.011	0.229	0.047	0.488	0.928

The PROMETHEE II results for Problem 2 clearly point to PO2-C as the best-performing option, with PO2-A a solid second and PO2-B consistently weakest. Under equal weighting, all options improve on the baseline (–0.333 at impact level; –0.213 at sub-impacts), but PO2-C achieves the highest net flows both at the impact level and sub-impact (0.333 and 0.162), ahead of PO2-A (0.000 and 0.130) and PO2-B (0.000 and –0.079). When the Problem 2 weighting is applied, this ordering becomes even clearer: PO2-C again records the highest net flows (0.333 at impact level and 0.443 at sub-impacts), PO2-A remains positive at sub-impact level but more moderate (0.150) and becomes negative at impact level (-0.133), performing worse than the baseline. Similarly, PO2-B is negative at the impact level and sub-impact (–0.400, - 0.072 at sub-impacts) and therefore appears poorly aligned with the sovereignty- and resilience-focused P2 priorities.

Thus, PROMETHEE II indicates that PO2-C offers the strongest and most robust performance across both impact and sub-impact structures, with PO2-A preferable to the baseline in most cases, and PO2-B clearly the least attractive option.

Table 59. PROMETHEE II - Problem 2 (Source: Technopolis et al. (2025))

Option	EW - Impacts	EW Sub-impacts	P2 - Impacts	P2 – Sub-Impacts
Baseline	-0.333	-0.213	0.200	-0.521
PO2-A	0.000	0.130	-0.133	0.150
PO2-B	0.000	-0.079	-0.400	-0.072
PO2-C	0.333	0.162	0.333	0.443

For Problem 2, ELECTRE III at the impact level, under both equal weighting and the P2 weights, the descending ranking is PO2-C > PO2-A = baseline = PO2-B. PO2-C is the only option that outranks all the other options and the baseline. At the sub-impact level, PO2-C again dominates in both EW and P2 options the ordering is PO2-C > PO2-A = baseline = PO2-B, with credibility values close to 1 for the outranking of the other options. This means that, when non-compensatory logic is applied and deal-breaker criteria are allowed to veto weak options, PO2-C is the clearly preferred option for Problem 2, while PO2-A and PO2-B offer at best a marginal improvement over the status quo. Within the second group of options, PO2-C generates a meaningful improvement relative to the status quo, while PO2-A and PO2-B do not materially change outcomes compared to the baseline.

Table 60. ELECTRE III ranking of options – Problem 2 (Source: Technopolis et al. (2025))

Option	Impact level (EW)	Sub-impact level (EW)	Impact level (P1)	Sub-impact level (P1)	Overall ELECTRE III judgement
PO2-C	1	1	1	1	Clearly strongest
PO2-A	2 = Baseline = PO2-B	2 = Baseline = PO2-B	2 = Baseline = PO2-B	2 = Baseline = PO2-B	At best marginal over baseline
PO2-B	2 = Baseline = PO2-A	2 = Baseline = PO2-A	2 = Baseline = PO2-A	2 = Baseline = PO2-A	At best marginal over baseline
Baseline	2 = PO2-B = PO2-A	2 = PO2-B = PO2-A	2 = PO2-B = PO2-A	2 = PO2-B = PO2-A	Reference

Stakeholder analysis

For economic operators, all three Problem 2 options deliver a clear improvement over the baseline, but with different strengths. Under equal weighting, PO2C clearly dominates PO2A and PO2B (0.552 vs 0.453 vs 0.421), reflecting that transparency measures and coordinated EU frameworks are seen as offering broad benefits even if costs remain mildly negative. When the Problem 2 weighting is applied, PO2C again becomes the standout option (0.851 vs 0.634 for PO2B and 0.611 for PO2A). This is driven by the fact that PO2C combines the strongest cost outcome for operators (costs shift from negative at baseline to clearly positive (0.036) with robust effectiveness and social gains. PO2-A still delivers the highest social score for operators (0.051) under EW and P2, but its weaker cost performance means it ranks second overall once the higher weight on effectiveness and cost dimensions is considered.

For national public authorities, preferences differ. All options again improve substantially on the baseline, but PO2-C is the most attractive option when judged against the Problem 2 priorities. This is mostly drive by its cost performance, which outranks the other options and the baseline. Under equal weighting, PO2-B already has the highest total score (0.215 vs 0.184 for PO2A and 0.136 for PO2C), largely because it nearly eliminates the negative cost gap while improving effectiveness and social outcomes. Under the P2 weighting, PO2B's advantage becomes less pronounced than PO2-C, which improves cost burdens for public authorities with respect to the baseline. By contrast, even though it outranks the other options across all dimensions under P2 weights, PO2-A leaves authorities facing notable net costs, which lowers its overall impact. In short, operators tend to strongly favour the EU-coordinated support package in PO2-C, whereas public authorities place greater value on PO2-C than PO2-B, specifically when applying P2 impacts, focused on digital sovereignty and resilience in the public sector including through public procurement.

Table 61 Economic Operators and Public Authorities MAUT – Problem 2 (Source: Technopolis et al. (2025))

Impact	Costs		Effectiveness		Environmental		Social		Total	
Economic Operators										
Option	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**
Baseline – P2	-0.369	-0.563	0.260	0.375	-0.038	-0.008	-0.003	-0.006	-0.149	-0.201
PO2-A	-0.074	-0.044	0.244	0.597	0.036	0.007	0.247	0.051	0.453	0.611
PO2-B	-0.009	0.113	0.181	0.474	0.036	0.007	0.195	0.040	0.421	0.634
PO2-C	0.036	0.180	0.238	0.615	0.045	0.009	0.234	0.047	0.552	0.851

National Public Authorities										
Option	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**
Baseline – P2	-0.318	-0.475	0.143	0.053	-0.125	-0.025	0.000	0.004	-0.300	-0.443
PO2-A	-0.153	-0.180	0.157	0.392	-0.016	-0.003	0.195	0.039	0.184	0.247
PO2-B	-0.024	0.075	0.146	0.318	-0.022	-0.004	0.116	0.023	0.215	0.413
PO2-C	-0.030	0.111	0.129	0.307	-0.025	-0.005	0.063	0.013	0.136	0.425

For CSPs and AI service providers under Problem 2, the MAUT results show that all three options perform markedly better than the baseline, but PO2-C emerges as the best-performing configuration overall. The baseline records negative total scores under both equal weighting (–0.102) and the Problem 2 weighting (–0.205), driven by cost penalties and limited effectiveness and social effects. Under equal weighting, total scores improve to 0.411 for PO2-A, 0.392 for PO2-B and 0.509 for PO2-C. When the Problem 2 weighting is applied the results are further confirmed. PO2-C becomes the clear leader with a total of 0.812, ahead of PO2-B (0.601) and PO2-A (0.567), while PO-A still performs well in terms of effectiveness and social outcomes.

For SMEs[105] results indicate that all three options improve substantially on the baseline, with PO2-C as the most favourable option under P2 weights and PO1-A under EW. Under equal weighting, all options outperform the baseline, with 0.508 for PO2-A, 0.499 for PO2-C and 0.394 for PO2-B, mainly by increasing effectiveness, social and environmental scores. When the Problem 2 weighting is applied, the contrast with the baseline becomes weaker: the baseline total increases to 0.352, while PO2-C reaches 0.723, compared with 0.653 for PO2-A and 0.518 for PO2-B. In this scenario, PO2-C combines clearly better cost outcomes and environmental impact, despite PO2-A has a slightly higher effectiveness and social score, indicating that more ambitious measures offer SMEs the most advantageous balance under Problem 2.

Table 62. MCDA Cloud and AI Computing Service Providers and Data Centre Operators MAUT – Problem 2 (Source: Technopolis et al. (2025))

Impact	**Costs**		**Effectiveness**		**Environmental**		**Social**		**Total**	
Cloud and AI Computing Service Providers										
Option	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**
Baseline – P2	-0.369	-0.563	0.262	0.363	-0.026	-0.005	0.031	0.000	-0.102	-0.205
PO2-A	-0.074	-0.044	0.229	0.559	0.026	0.005	0.229	0.047	0.411	0.567
PO2-B	0.009	0.113	0.171	0.445	0.029	0.006	0.183	0.037	0.392	0.601
PO2-C	0.036	0.180	0.225	0.582	0.033	0.007	0.215	0.044	0.509	0.812
SMEs										
Option	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**	**EW**	**P2**
Baseline - P2	0.000	0.000	0.233	0.346	-0.039	-0.008	-0.028	-0.013	0.166	0.325
PO2-A	0.000	0.000	0.237	0.598	0.038	0.008	0.233	0.048	0.508	0.653
PO2-B	0.000	0.000	0.174	0.473	0.034	0.007	0.186	0.038	0.394	0.518
PO2-C	0.030	0.092	0.217	0.580	0.043	0.009	0.210	0.043	0.499	0.723

7. ENVIRONMENTAL IMPACT ANALYSIS

The analysis of the environmental impact of data centres estimates the operational electricity consumption and associated CO_2 emissions of projected data centre capacity in the EU over the

[105] SMEs account for cloud and AI computing service providers.

period 2025-2036 under the baseline and the three different policy options (PO1-A, PO1-B and PO1-C). The calculation proceeded in four steps:

1. Use of installed IT capacity forecast under the baseline and the respective policy options (MW)
2. Adjustment for utilisation and efficiency
3. Conversion of electricity demand into TWh
4. Application of EU electricity emission factors to derive CO_2 emissions[106]

7.1. Installed IT capacity

Annual projections of maximum IT power draw (MW) are taken as the starting point for each scenario (Baseline, PO1-A, PO1-B, PO1-C), reflecting different trajectories of data centre deployment. Public sector capacity is tracked separately but aggregated into total capacity for environmental calculations. These projections imply compound annual growth rates of approximately: 11% (Baseline); 12% (PO1-A); 13% (PO1-C); 15% (PO1-B)

7.2. Utilisation and efficiency assumptions

Installed IT capacity is converted into effective operational load using a utilisation factor of 63%, reflecting the weighted average of data centre utilisation rates reported by Technopolis et al. (2025). These rates came from the CATI survey for colocation providers in primary markets (coming out at 50% utilised), with desk research used to calculate the utilisation rate for colocation providers in secondary and developing markets (45%) and hyperscaler sites (90% utilised). This yields the “effective IT load” for each year and scenario.

Power Usage Effectiveness (PUE). Colocation PUE was calculated using information from Data Center Map (coming out an overall average of 1.39) whereas hyperscaler PUE was calculated using the latest reported hyperscaler figures for their EMEA sites from 2023 (coming out at an average of 1.1). These figures were validated against market participants during interview programmes and during both the interim and final workshop. Total facility electricity demand is derived using scenario-specific PUE trajectories:

- Baseline improves gradually from 1.29 in 2025 to 1.23 in 2036
- PO1 scenarios assume faster efficiency improvements, reaching: 1.18 (PO1-A), 1.12 (PO1-B), 1.05 (PO1-C) by 2036

These assumptions reflect accelerated uptake of efficient cooling, infrastructure optimisation, and best-available technologies under policy intervention. For further details see section 2.3.4.

Total electrical load is therefore calculated as: *Total DC load = Effective IT load × PUE*

This produces declining electricity intensity per GW over time (TWh/GW), even as total consumption increases due to capacity growth.

7.3. Conversion to annual electricity demand

Electricity consumption is computed using the standard conversion:

Annual electricity (TWh) = Load (GW) × 8,760 hours × 0.001, equivalently: MW × 0.00876 = TWh/year.

This yields total annual electricity demand for each scenario, rising from approximately 99 TWh in 2025 to: 314 TWh (Baseline), 339–340 TWh (PO1-A / PO1-C), 408 TWh (PO1-B) by

[106] All policy scenarios use the same grid decarbonisation trajectories. Differences in emissions therefore arise exclusively from differences in compute deployment and efficiency.

2036. Cumulative electricity demand over 2025–2036 ranges from 2 571 TWh (Baseline) to 3 028 TWh (PO1-B).

7.4. Emissions calculations

Electricity consumption is translated into CO_2 emissions using EU-average electricity emission factors from the European Environment Agency. The emission factor declines from 0.25 kg CO_2e/kWh in 2025 to 0.16 kg CO_2e/kWh in 2036, reflecting projected grid decarbonisation[107]. Annual emissions are calculated as: CO_2 emissions (Mt) = Electricity demand (TWh) × Emission factor (Mt/TWh). The same emission factor trajectory is applied across all scenarios.

Despite improving energy efficiency (declining PUE and falling emissions per GW), total emissions increase due to strong capacity growth. By 2036 baseline annual emissions are expected to reach 50 Mt CO_2, PO1-A / PO1-C around 54 Mt CO_2, PO1-B reaches 65 Mt CO_2 At the same time, emissions intensity per GW declines by 41–49% across scenarios, illustrating that efficiency and grid decarbonisation partially offset, but do not fully neutralise the impact of capacity expansion. Efficiency improvements substantially reduce emissions per unit of compute. However, rapid expansion of data centre capacity dominates overall outcomes. Policy scenarios that accelerate deployment without parallel structural decarbonisation of power supply materially increase absolute emissions. This highlights the importance of coordinating compute expansion with grid investment and clean generation.

7.5. Limitations

This assessment provides an order-of-magnitude estimate of operational electricity demand and associated CO_2 emissions from projected EU data centre capacity. Several limitations should be noted:

- The analysis covers operational electricity consumption (Scope 2 emissions) only. Embodied emissions from construction, hardware manufacturing, and network infrastructure are not included. Life-cycle studies indicate these can be material, particularly during rapid build-out phases, meaning total climate impacts are likely understated.
- EU average grid emission factors are applied uniformly across scenarios. In practice, incremental electricity demand from new data centres may be met by marginal generation sources that differ from the average mix, possibly leading to higher or lower real-world emissions. A constant utilisation rate is also assumed across scenarios and years. Actual utilisation can vary widely over the asset lifecycle, which introduces uncertainty into absolute electricity estimates.
- Power Usage Effectiveness improvements are modelled as smooth, deterministic paths. Real-world efficiency gains depend on site-specific factors (climate, cooling technology, density, heat reuse) and may be slower or more uneven than assumed, particularly for retrofit facilities.
- The methodology does not distinguish between Member States or regions. Local grid carbon intensity, cooling requirements, and permitting constraints can substantially affect environmental outcomes, but are not captured in this EU-wide aggregate approach.

[107] 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)

Taken together, these limitations mean results should be interpreted as indicative ranges rather than precise forecasts, and primarily as a tool for comparing scenarios on a consistent methodological basis.

8. SO3 – How realistic is it to set an objective for EU providers to reach a market share of 30% by 2035?

Specific objective 3 sets the objective that, by 2035, this intervention should increase the market share of European cloud and AI computing service providers in the European market to 30%. The figure is not used for further calculation in this assessment, but it is worth reflecting on whether this is realistic altogether: what would it take for this figure to become reality?

A first element is that cloud adoption varies significantly depending on the user. According to Eurostat the adoption of cloud by businesses in 2023 is estimated at 45.2%, but while around 78% of the large enterprises use cloud services, only 59% of medium ones and 41.7% of small organisations have adopted cloud[108]. The level of adoption of cloud in the public sector was estimated at 30% in the context of PM15 and PM21. This gives a sense of where non-cloudified markets are and which ones offer the biggest potential for EU providers to gain new markets and improve their market share overall.

Looking at the different categories:

- Large customers could display a modest increase in the use of EU suppliers, causing the EU market share to grow by 3.5% CAGR for this segment. Large organisations, such as banks, telcos, IT or the manufacturing sector, are global industries that need to ensure service continuity around the world and will, for an ample part, retain international providers who can offer such geographic coverage: they are expected. Growth drivers for EU providers include, for example, multi-cloud strategies, reduction of vendor lock-in, and the shift towards sovereign solutions, especially for the more critical workloads. to be among the largest drivers in cloud expenditures in the following years[109]. For instance, some sources estimate the cloud expenditure in the banking and financial sector accounts for 27% of the overall market expenditure in the EU[110]. Other large customers, who are less global such as the aeronautic sector are moving their critical workloads to sovereign cloud services[111].

- SMEs could show a steady and more pronounced increase in the use of EU suppliers, causing the EU market share to grow by 7% CAGR, driven by the fact that a large percentage of SMEs are not yet on the cloud. With only 42 – 59% of SMEs (depending on the size) having adopted cloud, SMEs represent a large greenfield opportunity for EU cloud providers. Key enablers are lower switching costs and price sensitivity favouring regional providers. To this end, the SME programme (PM23) can act as real catalysers. Some companies like Odoo, a SaaS company offering a broad range of Open Source enterprise applications, are specialised in this type of market.

- The public sector could increase their use of EU suppliers much more rapidly, causing the EU market share to grow by 15% CAGR. This reflects the potential impact of joint procurement practices as well as procurement of sovereign services. This sector exhibits

---

[108] European Commission, Cloud Computing
[109] IDC
[110] Dimension market research
[111] See Airbus

the strongest sovereignty imperative with directly applicable policy levers, such as public procurement measures, sovereignty concerns, and NIS2 compliance, among others.

Warning: the respective CAGR, though presented with plausible explanations, have been picked to broadly match the desired outcome. The figures are presented to show a plausible evolution, and do not constitute a forecast.

Synergy puts today's market share of EU providers at 15%, a figure which, for the sake of this exercise, it is assumed to be the same across all three segments. The evolutions over the three segments would see the EU share grow as follows:

Table 67. European Cloud and AI computing service providers share of revenues - per customer segment (%)[112]

Segment	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Large enterprises	15.0	15.5	16.1	16.6	17.2	17.8	18.4	19.1	19.8	20.4	21.2
SMEs	15.0	16.1	17.2	18.4	19.7	21.0	22.5	24.1	25.8	27.6	29.5
Public sector	15.0	17.1	19.5	22.2	25.3	28.9	32.9	37.5	42.8	48.8	55.6

Today's cloud market is assumed to be divided into three segments: large customers (LC) amounting for 60% of the market[113], small and medium enterprises (SME) being around 26% and the public sector (PS) 14% of the market. Assuming this distribution remains the same, the share of the market for EU providers could evolve as follows:

Table 67. European Cloud and AI computing service providers share of revenues – aggregated (%)

Segment	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Total Share	15.0	15.9	16.8	17.9	19.0	20.2	21.5	23.0	24.5	26.3	28.2

[112] Shares indicate the proportion of cloud spend by each customer segment captured by European providers. Projections reflect assumed growth in sovereign demand, procurement preferences in the public sector, and gradual diversification of enterprise cloud sourcing. Total EU share is weighted by segment revenues.

[113] This is in line with what several sources estimate of the cloud market share for large organisations in Europe. See for instance GMInsights

9. Types of procedures, permits and data centre deployment timelines per Member State

Table 68. Types of permits and timeline per MS selected (Source: Technopolis et al. (2025))

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
Czech Republic Prague[115] [116] [117]	• Zoning and land allocation for a data centre in Prague generally takes 6-12 months • The city's zoning plan is updated quarterly or semi-annually. Incorporating changes into the valid zoning plan typically takes 1.5–2 months after approval by the city council	From submission to the relevant Building Authority (stavební úřad) for general construction works to decision and issuance, it takes 6-12 months	2 to 4 years for medium-sized projects, but can extend to 5 years or more for large-scale or high-capacity facilities	• Integrated into the permitting procedure under the new Building Act (effective July 2024) • EIA is required for large urban/industrial projects; national screening applies based on size/impact • Screening and scoping take 30 days and the public consultation about 30 days. Then, the EIA authority issues a binding opinion on environmental impacts, which is incorporated into the joint building permit (~10 months total)	24 - 60

[114] When it comes to grid connection procedures, 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. It also sets basic rules for third party access to electricity infrastructure in a non-discriminatory and transparent manner, applicable to all grid users, including DCs.

[115] https://geoportalpraha.cz/en/data-and-services/articles-and-projects/uzemni-plan

[116] https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/czech-republic

[117] https://www.czechbusinessguide.com/content-of-book-permitting-construction-permitting-processes/

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
Estonia Tallinn[118] [119] [120] [121] [122]	• If a detailed spatial plan is required <3 years • If only design specifications are needed ~30 days	From submission to the Tallinn Urban Planning Department to approval it takes 2-6 months	• For standard/small connection (<2 MW) it takes 6–12 months • For large-scale/hyperscale projects (>10 MW), it can take 1–3 years or more	• The EIA is integrated into the permitting process, and its approval is a prerequisite for the building permit • The need for an EIA follows the EU EIA Directive: screening for Annex II projects (urban development/industrial zones) • If needed, the Environmental Board (Ministry of Environment for large projects) determines if an EIA is required (30 days), the scoping and EI study take 6-12 months. Then there is a public consultation (30 days) and the approval comes 3-6 months after it • The developer then must submit again the building permit application to the local municipality after EIA approval (1-3 months in practice) • Total duration is 11-24 months	6-24

[118] https://www.tallinn.ee/en/ettevotjale/spatial-planning-procedures-and-timelines
[119] https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/estonia
[120] Data collected through interviews
[121] https://www.datacentermap.com/estonia/tallinn/datahouse@tallinn/
[122] https://investinestonia.com/estonia-has-the-most-advanced-data-center-in-the-region/

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
France Paris[123] [124] [125] [126] [127]	• If the land is already zoned for warehouse/data centre use, allocation takes weeks to months • If a zoning change is needed: 12–18+ months • Large projects require additional regional approval, adding up to 3 months	• From the application electronically to the Paris City Hall (Basu office) to approval takes average 3-6 months • If the project triggers environmental thresholds, an EIA is required by DRIEAT (Regional Directorate for the Environment, Planning, and Housing), bringing up the duration to 6-18 months	• Standard grid connections with RTE/Enedis takes 1.5–3 years • On utility-ready/pre-connected sites, time is under 1.5 years • For large or complex projects timeline may exceed 3 years	• EIA must be done before the building permit is granted, if required • EIA is required if emergency generators exceed 50 MW thermal output • Initial screening takes 1 month, whereas the EI study preparation takes 612 months • Once the public consultation starts (30 days), the approval comes 3-6 months after • After EIA approval, the developer submits the building permit application to Basu office • Total duration is 13-32 months	24 - 60
Germany Frankfurt[128] [129] [130] [131]	• Specific "suitability areas" (e.g., Sossenheim, Rödelheim, Griesheim, Gallus, Ostend,	• From the consultation with the City Planning Department (Stadtplanungsamt) and the Construction Supervisory	• Average waiting time for a new grid connection in Frankfurt (and for Germany)) is up to 7 years	• The EIA is integrated into the building permit process and must be completed before the permit is granted	24 - 84

[123123123] https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/france
[124] https://en.institutparisregion.fr/resources/publications/data-center-growth-and-proposals-for-regulation/
[125] https://www.linkedin.com/posts/stephanieelkhoury_datacentres-energy-connection-activity-7329060095772856320-ubcp
[126] https://en.institutparisregion.fr/fileadmin/NewEtudes/000pack4/Etude_3025/Etude-DataCenter-english_2023_VF.pdf
[127] https://www.edf.fr/sites/groupe/files/epresspack/9635/PR-Data-center-Vdef-1.pdf
[128] https://frankfurt.de/english/service-and-city-hall/service-and-administration/municipal-offices/city-planning-department/construction-advisory-services
[129] https://www.germandatacenters.com/en/news-en/detail/figures-of-the-month-data-center-ecosystem-germany-may-2025/
[130] https://www.lw.com/en/insights/energy-infrastructure-insights-data-centres-in-frankfurt-a-city-fit-for-the-future
[131] https://www.dlapiper.com/en/insights/publications/real-estate-gazette/real-estate-gazette-infrastructure/power-grid-connections-for-data-centers-in-germany

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
	Fechenheim, Seckbach) where company-independent (cloud/colocation) data centres can be developed (outside these areas, new data centres are not permitted) • If land is not zoned or is in a restricted/exclusion area (usually the case) a change or amendment to the development plan (Bebauungsplan) is required • Amending or creating a new development plan involves public consultation, environmental review, and approval by city authorities, governed by the German Building Code (BauGB) • Timeline is 6-12 months if there is land available in a suitability area and 1-2 years if a zoning plan amendment is required	Office (Bauaufsicht) to approval, most German states require the building permit to be granted within 6 months • 6–12 months is typical for well-prepared, straightforward projects in designated data centre zones • More complex or incomplete applications, or those requiring additional permits or plan amendments, can take up to 12–18 months	• Only if grid connection has been pre-secured in suitability areas, it can take 6-12 months	• EIA is triggered if backup generators exceed 50 MW thermal capacity • If required, the steps involved screening (1-2 months), scoping and EIA report (6-12 months depending on complexity), public consultation (30 days), EIA approval (by the regional environmental authority, 3-6 months). • After EIA approval, the developer submits the building permit application to the Frankfurt Construction Supervisory Office (Bauaufsicht) • The total timeline is 16-38 months	

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
Greece Athens[132] [133] [134]	• 6–12 months is typical for site selection and confirming zoning if the site selected is suitable (industrial use) • If zoning change or plan amendment is needed, timeline is 12–24 months	• The entire application and issuance process is electronic via the TEE e-permit platform • 2-6 months is typical for the building permit to be issued, provided all documentation is complete and the site is already zoned for data centre use • The process can take 6-12 months or longer, especially if the site is in a sensitive area (archaeological or environmental assessments), or if documentation is incomplete or needs revision	• Request must be submitted to the Independent Power Transmission Operator (IPTO/ΑΔΜΗΕ) for high-voltage connections, or to the Hellenic Electricity Distribution Network Operator (HEDNO/ΔΕΔΔΗΕ) for lower voltage • For most new data centre projects in Athens, the grid connection process—including application, technical studies, permitting, construction of substations or upgrades, and final commissioning—takes between 12-36 months • For hyperscale or high-capacity data centres (e.g., 100 MW+), the timeline can be closer to the upper end (2–3 years)	• The EIA is a prerequisite for the building permit. The building permit application cannot proceed until the EIA is approved • Data centres with ≥2 MW capacity fall under environmental regulations and EIA is likely to be triggered if capacity is ≥20 MW • The Ministry of Environment and Energy determines if an EIA is required based on project size, location, and potential impacts (1-2 months) • The following steps include scoping (1-3 months), EIA report (6-12 months), public consultation (1-3 months) and approval (3-6 months post-consultation) • Total timeline is 14-32 months	18 - 56

[132] https://en.mitos.gov.gr/index.php/%CE%94%CE%94:Issue_of_Building_Permits_(e-adeies)
[133] https://inconde.com/building-permits-in-greece/
[134] https://en.mitos.gov.gr/index.php/%CE%94%CE%94:Issue_of_Building_Permits_(e-adeies)

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
Ireland Dublin[135] [136] [137] [138] [139] [140] [141] [142]	• If the land is already zoned, it takes 6–12 months for site selection, plus 2–4 months for planning permission • If a zoning change is required, the process can extend to 1–2 years or more • Most new data centres in Dublin are built on pre-zoned "HT – High Technology" or industrial lands	Obtaining a building permit with the Dublin city Council takes 2–4 months for planning permission (longer if appeals or further information are needed), with building control certificates adding another 2–3 months (often overlapping with construction preparation)	• Since late 2021, EirGrid (Ireland's transmission system operator) has imposed a de facto moratorium on new data centre grid connections in the Dublin area (till 2028) • Outside Dublin, the connection take's 1-3 years (new policy from The Commission for Regulation of Utilities, CRU)	• The EIA is a mandatory part of the planning process and must be completed before a building permit (planning permission) is granted • A GHG permit required for generators >20 MW and a full EIA is typically required for larger projects • Screening is performed by the Dublin City Council, followed by the preparation of the EI report (6-12 months), public consultation (1-3 months) and final decision (8 weeks statutory timeline) • Total timeline is 10-24 months	• 24 (fastest case, out of Dublin) • Indetermined for Dublin
Italy	• If land already zoned for data centre use: 6–8 months (with due diligence and planning approval)	• Permitting and approvals (planning + building permit) takes in average 6–18 months • If the site is already zoned and documentation is complete,	• Standard grid connection: 2 to 4 years, due to a single national grid operator (Terna) processing all	• The EIA is a prerequisite for the building permit • EIA is required for generators >50 MW thermal output or for	24 - 60

[135] https://consult.fingal.ie/en/system/files/materials/22444/26992/BMC%20Vantage%20FCC%20Dev%20Plan.pdf
[136] https://www.dublincity.ie/residential/planning/planning-applications/make-planning-application/planning-process-application/planning-application-timelines
[137] https://www.dublincity.ie/residential/planning/planning-applications/make-planning-application/planning-process-application/about-planning-process-application
[138] https://www.mhc.ie/latest/insights/permitting-irish-data-centres-what-you-need-to-know-1
[139] https://www.dublincity.ie/residential/planning/building-control/about-building-control
[140] https://www.rte.ie/news/business/2022/0116/1273819-data-centres-eirgrid/
[141] https://www.capacitymedia.com/article/29ot42ikril15nn8s4c2t/news/new-data-centres-in-dublin-face-power-connection-delay
[142] https://www.bisnow.com/dublin/news/data-center/regulator-opens-up-possible-data-centre-pathway-amid-fears-dublin-has-been-left-behind-129587

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
Milan[143] [144] [145] [146]	• If zoning change or a plan amendment is needed (12–18+ months) • Brownfield site (with zoning) can happen in 6–8 months (incentive)	the process can be on the shorter end (6–8 months) • If zoning changes or complex planning are required: 12–18 months	requests, a large backlog and the need for upgrades • Brownfield sites, pre-zoned or fast track projects can get the connection in 1.5-2 years • On the other hand, large/complex projects can take 3-5 years	a total project capacity >150 MW • The Municipality of Milan determines the requirement (1-3 months) and, from there, the preparation, public consultation, approval and building permit review can add up to 17-32 months	
Netherlands Amsterdam[147] [148] [149] [150] [151] [152]	• If the land is already zoned and available: 2–6 months (plus site due diligence) • If a zoning plan amendment is required: 6–12+ months • Most new data centre developments are subject to strict municipal controls and sustainability requirements	• If the site is already zoned for data centre use: 8–14 weeks; with an environmental permit (≥15 MW), allow up to 26 weeks • If a zoning amendment or deviation is needed: 6–12+ months added before the permit can be reviewed • All projects must comply with the Environmental Act (Omgevingswet), including	• No new grid connections for data centres in Amsterdam are expected before 2030 unless the project is essential for the city and meets strict criteria • Even fully built data centres may remain idle if they lack a pre-secured grid connection. • Outside Amsterdam e.g., Rotterdam, Westland, grid	• The EIA process is integrated into the permitting framework and cannot be conducted in parallel with the building permit • An environmental permit is required at 15 MW and a full EIA is likely for larger hyperscale projects (>70 MW) • The competent authority (municipality or Omgevingsdienst	• 12 (fastest possible case, out of Amsterdam) • Indetermined for Amsterdam

143 https://www.assoimmobiliare.it/wp-content/uploads/2024/03/Colliers_Data-Center-Snapshot-2024_Italy__.pdf
144 https://datacentrenews.uk/story/virtus-announces-new-data-centre-plans-for-milan-italy
145 https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/05/data-centres-in-italy.pdf
146 https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/italy
147 https://www.stibbe.com/publications-and-insights/increasing-control-of-data-centre-locations
148 https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/netherlands
149 https://cms-lawnow.com/en/ealerts/2022/11/netherlands-prohibits-creating-hyperscale-data-centres-until-national-guidelines-are-passed
150 https://openresearch.amsterdam/image/2020/4/30/the_governance_of_land_use_amsterdam_2017.pdf
151 https://www.haskoning.com/en/newsroom/blogs/2023/navigating-dutch-data-centre-challenges-and-opportunities
152 https://www.portofamsterdam.com/sites/default/files/2020-06/guide-permit-application.pdf

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
	• For hyperscale data centres (>10 hectares/70 MW): New developments are effectively banned in Amsterdam and most of the Netherlands	energy efficiency and emissions standards • Engaging with the city and OD NZKG early can clarify requirements and avoid delays	connection is possible within 1–3 years	Noordzeekanaalgebied, OD NZKG, for larger projects) determines if an EIA is required, by submitting a screening request through the Omgevingsloket (environmental permit portal). This takes 1-3 months • The EI report, public consultation and building permit review in total take from 10-24 months	
Poland Warsaw[153] [154] [155] [156] [157] [158]	• If the site is already zoned: 1–2 months • If a zoning permit is needed: 3–9+ months • If an environmental decision is required: add up to 6 months. • Land acquisition can proceed in parallel, but legal title is needed before the building permit stage	• Obtaining a building permit takes 65 days to 6 months • The process is managed by the district authority (starosta)	• Starts by submitting request to the network operator (e.g., PGE Dystrybucja, Innogy Stoen Operator) • In general, the process takes from several months–1 year • Full grid connection (total process) is 2–3 years • In large projects (100 MW+) with major upgrades/delays: 3+ years	• The EIA is a mandatory preliminary step that must be finalized before applying for the building permit • The EIA requirement follows the EU EIA Directive and there is a screening for industrial projects based on size/impact • The screening is submitted to the Regional Environmental Protection Authority i.e., Mazovian Voivodeship and	24 - 45

[153] https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/poland
[154] https://www.legal500.com/developments/thought-leadership/a-planning-permit-can-be-obtained-in-poland-if-land-to-be-developed-is-located-within-a-development-zone/
[155] https://dwfgroup.com/en/news-and-insights/insights/2024/9/general-zoning-plan-for-warsaw
[156] https://consultant.net.pl/en/consultant-article/how-to-obtain-a-building-permit-in-poland-1
[157] https://www.gtlaw.com/en/insights/2024/4/data-centres-in-poland-planning-and-electricity
[158] https://natlawreview.com/article/data-centres-poland-planning-and-electricity

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
				from there, the total process can take 11-24 months	
Romania Bucharest[159] [160] [161] [162] [163] [164] [165] [166] [167]	• Zoning and land allocation for a data centre in Bucharest can take a few months for small plots (<3,000 sqm) with no PUZ (Zonal Urban Plan) required, or 3–6 months if a valid PUZ is already in place • For larger plots requiring a new PUZ, the process can take 1–2 years or more but is currently subject to major delays due to legal and administrative gridlock	• The Romanian Construction Law stipulates that building permits must be issued within 30 days. In practice, it takes 6-12 months • Building permits are issued by either the General Mayor of Bucharest or District Mayors, depending on project type and location	• Romania's energy regulator (ANRE) has recently overhauled grid connection rules. As of June 2025, only fully documented projects are placed in the queue, and developers must provide a financial guarantee before receiving a grid connection permit • Timeline is 1.5–3 years for grid connection, from application to energization.	• The EIA is a prerequisite for the building permit • The EIA requirement follows the EU EIA Directive and there is a screening for industrial projects based on size/impact • From sending the screening to the Bucharest Environmental Protection Agency, the total timeline for an EIA is 11-24 months	18 - 36
Spain	• The municipality determines the specific	• Granted based on the technical project submitted by the developer. 3-12 months (3-4	• Submitting an access and connection request to Red Eléctrica de España (REE),	• An Environmental Impact Assessment (EIA) may be required (e.g., projects > 15	12 - 48

[159] https://www.businessforum.ro/real-estate/20241129/investors-in-data-centers-enter-race-for-land-plots-in-romania-1111
[160] https://www.property-forum.eu/news/data-center-investors-enter-race-for-land-plots-in-romania/19253
[161] https://www.arl-international.com/sites/default/files/2023-11/Fact%20sheet%20for%20planning%20levels_local_Zonal%20Plan.pdf
[162] https://cms-lawnow.com/en/ealerts/2022/08/bucharest-tribunal-rules-against-the-city-s-main-zoning-plan
[163] https://buildecon.blog/2025/03/20/bucharests-drop-in-residential-permit-and-completion/
[164] https://www.cristinatudor.ro/en/post/unlocking-romania-s-building-permit-process-your-gateway-to-successful-construction-projects
[165] https://www.nglsymbio.com/wp-content/uploads/construction-permits-in-cee-practical-guide-1.pdf
[166] https://horizons.legal/wp-content/uploads/2025/02/CONSTRUCTION-PERMITS-IN-CEE-01-25-1.pdf
[167] https://www.pv-magazine.com/2025/06/16/romania-updates-grid-connection-rules/

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
Madrid[168] [169] [170] [171] [172]	planning designation (industrial use) • Amendments/new planning involves, detailed planning, municipal review, and sometimes higher-level regional approvals (6-12 months on top) • There are no land plans or zones that automatically authorise data centres in Madrid; approvals are granted on a case-by-case basis	months in straightforward cases) • First Occupancy License (Licencia de Primera Ocupación): obtained after construction, confirming the building complies with the building permit. Involves inspection by municipal officials (3-6 months). • Activity and Opening Licenses (Licencia de Actividad y Licencia de Apertura): confirms regulatory compliance for the intended use. "Declaración Responsable" (responsible declaration), the license is immediate or nearly immediate. For activities requiring a full license procedure (for significant or "qualified" activities), the	the national transmission system operator • Undergoing feasibility studies, technical reviews, and regulatory approvals • Construction of new substations or high-voltage lines if required • Final commissioning and energization • <12 months If the site is already near a substation with available capacity, or if a developer has pre-secured grid access • 2–4 years is the benchmark (especially for data centres > 100 MW)	MW), depending on the size and location of the project. This can add several months to the process, especially if public hearings or additional studies are needed • The average is 11-24 months, including the determination request, EI study, public consultation and DIA issuance) • DIA must be issued before the building permit is granted	

[168] CMS. (2025). Expert Guide on Real Estate Data Centre Consenting: Spain. Retrieved June 17, 2025, from https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/spain
[169] Aeclu. (n.d.). Cuánto tarda la licencia de primera ocupación en Madrid. Retrieved June 17, 2025, from https://www.aeclu.com/blog/noticias/cuanto-tarda-la-licencia-de-primera-ocupacion-en-madrid/
[170] Madrid Licencias. (n.d.). ¿Cuánto tarda una licencia de apertura y actividad? Retrieved June 17, 2025, from https://www.madridlicencias.com/blog/cuanto-tarda-una-licencia-de-apertura-y-actividad/
[171] Strategic Energy Europe. (n.d.). Spain DC: Centros de datos y renovables. Retrieved June 17, 2025, from https://strategicenergy.eu/spain-dc-centros-de-datos-y-renovables/
[172] Montel News. (2024, March 21). Spain power demand may get 3 GW boost from data centres. Retrieved June 17, 2025, from https://montelnews.com/news/db842f28-b5f8-4c75-b914-cfd2792d219a/spain-power-demand-may-get-3-gw-boost-from-data-centres

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
		process typically takes 3-6 months			
Sweden Stockholm[173] [174] [175] [176]	• Land designated as "technical facility" use in the municipal zoning plan (detaljplan): 0 months • If not, new/amended zoning plan is needed (municipal approval + public consultation): +12-24 months	• Building permit (bygglov) average is 2-3 months (may take longer for complex projects) • After approval, a "start clearance" is needed before construction can begin, and a final clearance before the facility can be used	• Initiated in parallel or even before the permitting process by engaging with local grid owner (often Ellevio or Vattenfall) • Technical and feasibility studies, land rights and permits, construction and commissioning take 2-4+ years	• Data centres themselves usually do not require a separate environmental permit (integrated within overall permitting) • if the project involves significant water use or heat recovery, additional environmental permissions may be needed (in line with the EU EIA directive) • The steps are screening and scoping (60 days), preparation of EI statement, submission and completeness check, public consultation (30 days). • The permit authority (often the Land and Environment Court or Environmental Assessment Delegation) may hold hearings or written consultations with all parties	• 24 (average case) • 48+ (worst possible case)

[173] CMS. (2025). Expert Guide on Real Estate Data Centre Consenting: Sweden. Retrieved June 17, 2025, from https://cms.law/en/int/expert-guides/cms-expert-guide-on-real-estate-data-centre-consenting/sweden

[174] City of Stockholm. (n.d.). Building permits in English. https://bygglov.stockholm/in-english/

[175] Node Pole. (n.d.). Node Pole Report (Sweden). https://8866495.fs1.hubspotusercontent-na1.net/hubfs/8866495/Node%20Pole%20Report%20(Sweden)%20-%20FINAL.pdf

[176] Rigord, N. (2024). EIA effectiveness in Sweden: a Stockholm case-study [Master's thesis, KTH Royal Institute of Technology]. DiVA Portal. http://www.diva-portal.org/smash/get/diva2:1898845/FULLTEXT01.pdf

	Zoning & land allocation	Building permit	Utilities & grid connection[114]	Environmental permit/s	Average timeline (months)
				• Timeline is 6-18 months and up to 24 months for complex cases • The building permit cannot be granted until the environmental permit (including the EIA) is in place	

ANNEX 5: COMPETITIVENESS CHECK

1. OVERVIEW OF IMPACTS ON COMPETITIVENESS

Dimensions of Competitiveness	Impact of the initiative (++ / + / 0 / - / -- / n.a.)	References to sub-sections of the main report or annexes
Cost and price competitiveness	+	Section 6.1.5, Annex 4
International competitiveness	+	Section 6.1.5, Section 6.1.6
Capacity to innovate	++	Section 6.1.1, Section 6.1.4
SME competitiveness	+	Section 6.1.1

SYNTHETIC ASSESSMENT

Cost and price competitiveness

CADA will impact both costs and price competitiveness. Building data centres is a capital-intensive and complex activity that requires multiple permits and investments in its whole lifecycle (design, construction and operation). The facilitation of access to land and streamlined grid connections along with fast-track permitting procedures is expected to reduce total cost of ownership for data centre operators (PO1-B). By shortening approval times, simplifying and harmonising requirements the cost of the immobilised capital as well as transaction costs will be lowered. The introduction of a national facilitator for data centre projects will allow to save administrative time, very important for SMEs. The result of the preferred package is expected to increase the number of providers, enhancing competition and reducing market concentration.

Under the preferred package (PM8 and PM9), research and innovation will fund novel technologies (e.g. advanced cooling, AI-based energy optimization, etc..) to achieve much more efficient data centres in terms of use of energy. This innovation is expected to have positive spillovers across the European cloud and AI value chain. Businesses benefitting from the development of such innovations can achieve a lower total cost of ownership (TCO), and transfer part of these gains to customers through more competitive pricing for access to data centre capacity. This is particularly important for EU companies as they operate at smaller economies of scale than their international counterparts.

With respect to cloud and AI computing services, PO2-C under the preferred package implies additional costs for cloud and AI computing service providers to be audited with a view of achieving a sovereignty qualification which allows for providing services to public administrations in highly critical use cases. This may result in an increase of prices for sovereign cloud and AI computing services, as the cost of adjusting (e.g. due to the creation of new legal constructs) may be passed on to the customers in the form of a price premium. This will be the case until the market has stabilised, and the providers have recuperated the investment undertaken (short-term). The risk sovereignty mechanism is expected to be an important cost aspect for SMEs due to the effort needed to obtain and maintain the audit. Over time, however, a harmonised and recognised mechanism valid across the EU will reduce transaction costs and increase trust and market access.

Joint procurement and federation are likely to have a two-fold cost impact. First, they will create economies of scale on the demand side, reducing unit prices for procured services. Second, they will generate predictable demand signals, which will decrease the risk premiums of the suppliers. Joint procurement and federation can reshape the market by creating a large pool of aggregated demand open to multiple providers, notably allowing smaller providers to compete for specialised services. This will result in an overall improved situation of the public sector using cloud and AI computing services, mitigating the risks stemming from dependence on a small number of providers. An additional element is transparency: through the access to large contracts, smaller cloud and AI computing service providers can retain customer acquisition costs (CAC) and amortise fixed development expenditures. This will result, in the medium term, in a more stable cost structure and greater price competitiveness.

The creation of a cloud and AI toolbox is expected to promote further competition by allowing European providers to better integrate their service offerings. Currently, there is a large fragmentation across national markets and cloud, and AI computing services are not comparable which create uncertainty. This is expected to have a positive impact in SMEs.

The directly affected sectors are data centre operators and the providers of cloud and AI computing services. While both sectors will need to undergo some adaptation in the way they work, this is not expected to not cause a disruption and will mostly result in benefits, such as savings in construction time, aggregated offers, and more security and resilience. Indirectly affected sectors are on one end of the value chain the public sector and the customers of the cloud and AI computing services market and on the other, the semiconductor industry, energy systems and utilities.

Cost-price impacts of the preferred package (PO1-B + PM8 + PM9 + PO2-C) are expected to be different depending on the problem driver targeted. Faster permitting and access to land as well as clear procurement criteria will cause effects in the short term (0-2 years). In the medium term (2-5 years), the effects will arise from the go-to-market of the research and innovation funds, the putting in place of the federation mechanisms, which will allow an intensification of competition, a decrease of prices and efficiency gains. Long-term impacts (>5 years) will come from the combination of selected locations for computing infrastructure and the access to energy and other natural resources, notably by gaining location advantage.

The preferred package shall notably improve competitiveness. It implies a learning curve to implement some of the policy measures proposed (e.g. energy efficiency technologies, research and innovation, federation, interoperability) and network effects (e.g. open source). However, one of the major risks is on the implementation of permitting and access to grid and how they are managed (e.g. sequentially, in parallel) as these have an effect on the structural costs and durable price competitiveness.

International competitiveness

CADA strengthens the competitive position of data centre operators active in the EU and of European cloud and AI computing service providers.

In the case of data centre operators, it will reduce structural cost disadvantages stemming from the fragmented permitting regimes existing nowadays (see Annex 4, section 8). Data centre operators in the EU will be able to expand their capacity faster at lower cost. Simplification of administrative procedures will reduce entry barriers, notably for mid-sized firms, favouring the scalability of European players (PM4, PM5). Both EU and non-EU players, however, will benefit from vast economies of scale.

The deployment of computing infrastructure across the EU, and notably the deployment of sovereign cloud and AI computing services, will allow the EU to decrease its dependencies on data infrastructure located outside of the EU and its dependence on non-European providers of cloud and AI computing services, while increasing the economic security of the EU in the field of cloud and AI. The creation of a common definition of sovereignty, with clear criteria, along with the mandatory sovereignty risk assessment (PM21), will boost the trust and credibility of sovereign services, allowing their providers to differentiate themselves in markets where security, sovereignty and compliance are key items. Providers of sovereign services will hence be able to compete on trust, transparency and robustness rather than on price alone.

The establishment of research and development funding, addressing technological asymmetries with global incumbents will allow to develop next-generation technologies for energy efficiency, AI and other aspects (PM8, PM9). Currently, non-EU providers often lead with proprietary solutions. The use, reuse and promotion of open source in public administrations, will accelerate innovation allowing EU companies to compete in terms of performance, energy efficiency, and novel offers (PM20).

All measures under this initiative are conceived to be in line with the EU's international trade obligations. The initiative looks to incentivise local investment and aggregate demand by anchor customers, ensuring that competitive advantage is grounded in trust and operational excellence rather than on market power.

Finally, the initiative seeks to enable European providers to gain market share at EU and international level, by equipping them with the necessary mechanisms to enhance the scale and scope of their service offering. In the mid to long term, the levers proposed in this initiative (e.g. fast-permitting, national facilitator, funding mechanisms, joint procurement, federation) to solve very clear challenges of today (e.g. sustainability, skills, leverage of open source, aggregation of demand, sovereignty) will allow European providers to expand their market presence, in the EU and beyond.

Capacity to innovate

CADA goes directly at the heart of improving the capacity to innovate (PM8, PM9) and the improvement of skills (PM23). The funding mechanisms (PM8, PM9), complemented with the cloud and AI adoption scheme targeted towards SMEs and the skills certification (PM23) will boost the capacity to innovate at product, service and process level. The spillover effects of research funds, where a myriad of EU stakeholders can participate (e.g. academia, SMEs, large enterprises), allow also for the initiative to anchor intellectual capital and innovation capabilities within the EU.

Other aspects such as the promotion of open source in the public sector enlarge the amount of resources available for future innovative products and services (PM20). Open source allows to balance open innovation with adequate intellectual property protection. EU public sector bodies are hence able to reuse and extend these solutions under clear legal certainty, lowering entry costs for smaller innovators.

Finally, the use of well-defined sovereign criteria (PM21) are expected to create a demand-pull effect in the market, where companies will invest in R&D in order to develop technologies that will equip them to meet these criteria in a more efficient way.

SME competitiveness

The initiative directly affects SMEs, mostly in a positive manner. By removing bureaucratic friction and accelerating permitting times, boosting innovation capacity and mechanisms to adopt or migrate to cloud and AI and allowing to share resources and services, the initiative levels the playing field between smaller and larger providers by reducing fixed regulatory costs that otherwise would deter SMEs from participating in the operation of data centres and the provision of cloud and AI computing services. The measures allow SMEs to compete on merits and specialization, not marketing budgets. The audit scheme, however, generates a burden for SMEs, both to obtain it and to renew it on a yearly basis. But this can have a double effect. First, since it will be valid throughout the EU, it may open new markets to providers that now are out of reach due to other requirements (e.g. national certification schemes or labels), notably in the context of public procurement. Second, being audited under clear sovereign criteria may be used by SME providers to capture part of the private sector market dealing with highly critical data (e.g. defence) and to overcome the buyers' bias towards solutions offered by larger providers.

The minimisation of the burden on SMEs is one of the goals of this intervention, as well as simplification, proportionality, harmonisation, supportive ecosystems and open access. All these considerations stay at the core of the initiative, by for instance, transforming compliance into an innovation catalyst, by providing compensatory enablers (e.g. grants, national support measures).

For more information see Annex 6 SME check.

ANNEX 6: SME CHECK

OVERVIEW OF IMPACTS ON SMES

Relevance for SMEs

Based on SME filter and the (first) ISG discussion, this initiative is **relevant** for SMEs[177]

(1) IDENTIFICATION OF AFFECTED BUSINESSES AND ASSESSMENT OF RELEVANCE

Are SMEs directly affected? In which sectors?

SMEs are directly affected, though in different ways depending on their role in the data centre, cloud and AI value chain. Firstly, on the limited and geographically concentrated availability of computing capacity (P1), the affected SMEs are those companies building and operating data centres, which encompass data centre operators, cloud service providers that build and operate their own data centres, construction and real estate companies. Building data centres is a capital-intensive activity and hence the number of SMEs affected is limited. Secondly, on the dependence on cloud and AI computing services supplied by non-European providers (P2) there are two strands of SMEs stakeholders affected by the current initiative. First, cloud and AI computing service providers, that is, those organizations that develop and offer their services to business and governmental customers and on the other, SMEs that use cloud and AI computing services.

Estimated number of directly affected SMEs

SMEs directly affected by the initiative, i.e. involved in building or operating data centres are approximately 150 across the EU[178]. Furthermore, the Technopolis et al. (2025) mapped[179] existing cloud service providers in the EU (284) and the results yielded that around 60% of the identified providers are SMEs or startups headquartered in the EU (175) whereas including non-EU headquartered, the number amounts to 200[180]. The same mapping exercise was carried out for AI service providers but the results to quantify the affected organizations are less conclusive.

Beyond cloud and AI computing service providers, the policy measures under consideration, notably the cloud and AI adoption scheme for SMEs, also affect ICT SME companies[181] (65 000) that wish to use cloud and AI computing services. More broadly,

---

[177] https://ec.europa.eu/docsroom/documents/63274.

[178] Technopolis et al. (2025), “Study: cloud and AI”

[179] The mapping carried out by Technopolis et al. (2025), “Study: Cloud and AI” included a manual search cross checked and complemented by existing market reports, entities participating in the Alliance for industrial data, edge and cloud, and MS reports (e.g. qualified entities by SecNumCloud).

[180] In contrast, the study identified 59 large cloud service providers headquartered in the EU.

[181] According to Eurostat, there are closed to 1.3 bn ICT companies, divided as follows: 1.2 bn are micro, 53,000 are of small size and 12,000 are of midsize. For this domain, only small and midsized companies have been taken into consideration.

SMEs in general (1.6 bn)[182] will also be affected by the broader availability of cloud and AI computing services, and through the cloud and AI adoption scheme.

Estimated number of employees in directly affected SMEs

The directly affected SMEs, i.e. those building or operating data centres and those who would increase their user of cloud and AI computing services, are likely employed between 50 and 250 people each, as they are typically small/medium-sized, highly specialised technology firms. With roughly 300 such SMEs across the EU, the total number of employees directly affected can be estimated at around 75.000 people EU-wide.

Are SMEs indirectly affected? In which sectors? What is the estimated number of indirectly affected SMEs and employees?

The value chain consists of three types of SMEs: data centre operators, cloud and AI computing service providers and cloud and AI computing service users. Service providers deploy their services on a data centre and offer the services to the user. Depending on the policy measure, service providers are either directly targeted or indirectly.

In the context of the first problem, the limited and geographically concentrated availability of computing capacity, the policy measures directly affect data centres operators and indirectly affect cloud and AI computing service provider. A broader availability of data centres will (indirectly) affect positively cloud and AI computing service providers as they will be less subject to a shortage of infrastructure where to deploy their applications and services or where they can train or inference their models. This is particularly the case for European SMEs leading in AI, which face significant challenges in obtaining the resources, funding, and market opportunities they need, often finding themselves pushed into early commercial dependencies with infrastructure providers. The number of cloud and AI computing service providers aligns with the values indicated above.

In the context of the second problem, the dependence on cloud and AI computing services supplied by non-European providers, the policy measures directly affect SMEs that provide cloud and AI computing services and indirectly affect those SMEs that use these services. Here, the extent of SMEs indirectly benefiting from an increase cloud and AI update is virtually all of them as for example such services are increasingly necessary to declare taxes, produce electronic bills or manage the day-to-day operations of a business, even for single persons' businesses. The same logic applies for the subset of SMEs that need sovereign cloud and AI computing services with a higher level of protection.

[182] SME Performance Review - Internal Market, Industry, Entrepreneurship and SMEs estimates the existence of 26 bn SMEs, out of which more than 24.5 bn are considered micro.

(2) CONSULTATION OF SME STAKEHOLDERS

How has the input from the SME community been taken into consideration?

Input from the SME community has been taken into consideration through the public consultations (survey and call for evidence), targeted consultations by the study team, stakeholder workshops, and continuous dialogue with industry associations, and innovators active in AI and cloud technologies. The following SME respondents have participated to the:

- Public consultation: 17 SMEs (or 25% of total business replies)
- Call for Evidence: 25 SMEs (or 45% of total business replies)
- Targeted consultations by the study team
- Stakeholder workshops
- Bilateral dialogues

Are SMEs' views different from those of large businesses?

Yes. SMEs' views differ significantly from those of large businesses, mainly due to their resource constraints, market position, and regulatory capacity. While large companies generally support stronger cloud and AI ecosystems, they often focus on scaling infrastructure, interoperability, and competitiveness at a global level. In contrast, SMEs emphasize accessibility, affordability, and simplicity as they need easier access to compute resources, clearer guidance on compliance, and reduced administrative and financial burdens.

(3) ASSESSMENT OF IMPACTS ON SMEs[183]
What are the estimated direct costs for SMEs of the preferred policy option?
Qualitative assessment
PO1-A improves SME access to information through clearer guidelines, reducing costs from information gaps and helping SMEs voice concerns collectively. PO1-B simplifies permitting, cutting legal and administrative burdens and lowering entry barriers to the data centre value chain. PO1-C has similar effects but may feel more distant due to EU-level approval; however, added public R&D and deployment funding strengthens SME participation in advanced projects without heavy capital needs. Potential direct administrative costs under the preferred policy option among these, i.e. PO1-B with PM8 and PM9, would be related to the time required to apply for EU or national funding support. PO2-A provides clarity on sovereign cloud and AI computing services without extra administrative load, while interoperability and the EU sovereignty conference boost SME visibility. PO2-B lowers verification costs via validity throughout the EU and supports SME cloud and AI adoption, with procurement criteria and vendor-neutral training improving SME competitiveness. PO2-C delivers the strongest benefits: although mandatory audit adds some cost, EU-wide validity expands market reach, open-source access reduces barriers, funding programmes favour SMEs. Overall, PO2-C and the SME cloud and AI adoption scheme enhance competitiveness, reduce upfront

[183] The costs and benefits data in this annex are consistent with the data in annex 3. The preferred option includes the mitigating measures listed in section 4.

costs, and support wider SME digital transformation. Similarly, as above, quantifiable administrative costs for SMEs stem from the time required to apply to receive funding under PM23.
Quantitative assessment
Under PM23, within PO2-C, SMEs are expected to incur in modest administrative costs related to their need to apply to receive the funding. The effort to prepare a project proposal is estimated to be 2 persons for 10 days (20 staff days), with total costs estimated at EUR 55 373 928 (NPV, 10-years), considering over 60,000 SMEs applying to receive funding.
What are the estimated direct benefits/cost savings for SMEs of the preferred policy option[184]?
Qualitative assessment
For PO1-B, SMEs would see direct benefits mainly through reduced legal, consultancy, and administrative costs. Streamlined permitting makes procedures easier to navigate, which cuts the time and external support SMEs typically need to comply with complex rules. Faster approvals also shorten project timelines, lowering costs and making market entry cheaper. With public funding under PM8 and PM9, SMEs save directly by reducing the upfront capital normally required for R&D, innovation, and deployment projects. Higher funding rates for SMEs lower financial risk and make participation in advanced initiatives more affordable. Funding also helps SMEs join larger consortia more easily, lowering the financial barriers to entering markets that typically favour large players. Under PO2-C, SMEs gain the largest net cost savings. Validity throughout the EU of audits means an SME audited in one Member State avoids repeating costly verification processes elsewhere. Support measures for adopting cloud and AI computing services lower training, integration, and compliance costs. Together, these reduce technology investment, administrative overhead, and business development expenses.
Quantitative assessment
Under PM23, within PO2-C, SMEs are expected to benefit directly from EUR 328 412 809. This policy measure puts forward a targeted scheme to provide financial support to SMEs for adopting cloud and AI computing services to increase their productivity and competitiveness. Most of the yearly budget considered for this measure, i.e. EUR 38.500.000, is dedicated to supporting the design and planning phase of cloud and AI-based transformation projects for SMEs. The grants are fixed amounts that the SMEs can spend in consultancy services to design digital transformation projects based on cloud and AI technology. The objective is reaching 2% of the small (10 to 50 employees) and midsize (50 to 250 employees) SMEs over the 10-year period. Every year, SMEs that have designed the most innovative cloud and AI-based transformation project plans will receive additional support to fund their implementation.
What are the indirect impacts of this initiative on SMEs?

[184] The direct benefits for SMEs can also be cost savings.

Most of the policy measures contribute to the development of European datacentre infrastructure and cloud computing capacity, a richer European cloud and AI computing service offering and a more dynamic technological and industrial ecosystem, contributing to a higher adoption of cloud. This will improve the efficiency in software and IT projects, increasing productivity of IT staff, ensuring the continuity of business processes (less downtime) and facilitating migration processes, for SMEs and large organizations alike. This impacts not only the efficiency of the IT staff but also the flexibility and capability of the European private sector to adapt in an agile way to evolving market needs and conditions, and to the dynamic technology landscape, increasing its competitiveness. This agility is particularly important for SMEs, who need to continuously adapt their technologies and business models in order to not lose market revenues and remain relevant.

This could have been measured in terms of effort saved in IT tasks (FTEs) but it would have been difficult to allocate the specific contribution for each specific measure, adding potential risk of double counting their effect.

SMEs outside the cloud sector also gain from a more trusted and interoperable EU cloud/AI ecosystem through safer access to digital tools, easier cross-border operations, enhanced innovation, and participation in data-driven markets. While quantification in some cases appears difficult, the qualitative impact of the initiative could be summarised as follows:

1. Access to Advanced Digital Services

Enhanced trust and interoperability in the EU cloud and AI market gives SMEs in other sectors access to advanced digital services. Businesses can safely and efficiently adopt cloud-based tools for e-commerce, logistics, HR, or data analytics, even if they are not part of the cloud industry itself.

2. Cross-Border Expansion

Standardised regulations and secure, cross-border data flows make it easier for SMEs to expand across Member States. Companies can scale products and services without facing legal or technical barriers, simplifying international operations within the Single Market.

3. Innovation through Collaboration

SMEs can integrate AI, IoT, or data-driven services into their offerings, driving modernization in traditional industries. Trusted cloud infrastructure lowers risks and investment barriers, enabling experimentation and digital transformation.

4. Cost Efficiency and Resilience

Reliable EU cloud services improve cost efficiency and resilience[185]. Reduced dependence on non-European providers decreases operational risks while competitive

[185] The adoption of AI and cloud technologies by SMEs can significantly boost economic performance. Some university studies indicate that AI adoption can increase revenue by up to 91% for SMEs, with operational costs potentially reduced by up to 30% and time savings exceeding 20 hours per month arXiv.

pricing and high availability could benefit sectors like manufacturing, healthcare, and fintech[186].

5. Participation in Sectoral Data Spaces

SMEs can participate in sectoral data spaces that provide shared datasets for areas like e.g. health, transport, energy, and finance[187]. Access to these resources opens opportunities for new products, services, and partnerships, fostering innovation and growth across the Single Market.

(4) MINIMISING NEGATIVE IMPACTS ON SMEs

Are SMEs disproportionately affected compared to large companies? No

If yes, are there any specific subgroups of SMEs more exposed than others? N/A

Have mitigating measures been included in the preferred option/proposal? Yes, financial support for SMEs to adopt cloud and AI (PM23)

CONTRIBUTION TO THE 35% BURDEN REDUCTION TARGET FOR SMEs

Are there any administrative cost savings relevant for the 35% burden reduction target for SMEs? SMEs are expected to benefit directly from PM23.

[186] Trusted cloud and AI adoption empowers SMEs across sectors: in manufacturing, AI improves operations and competitiveness (ScienceDirect); in healthcare, cloud solutions enhance patient experiences and administrative efficiency (ACE Cloud Hosting); and in fintech, AI tools support revenue forecasting, risk modelling, and financial decision-making (ResearchGate).

[187] In healthcare, AI enhances diagnostics and patient care, improving efficiency and outcomes; in transport, AI optimizes logistics and route planning, reducing costs and emissions; in energy, AI facilitates smart grid management and energy efficiency, supporting sustainability goals; and in finance, AI-driven tools assist in risk assessment and financial planning, enhancing decision-making capabilities. These advancements are supported by EU initiatives such as the Digital Europe Programme and Horizon Europe, which aim to bolster AI and digital infrastructure across the Union.

ANNEX 7: EXTERNAL COHERENCE WITH RELEVANT EU LEGISLATION AND POLICY INITIATIVES

For each Policy Option, the table below analyses its external coherence.

PO	External coherence
PO1-A	PM1 complements the existing Alliance for Industrial Data, Edge and Cloud. PM2 creates a permanent forum that currently does not exist. PM3 complements existing best practices that focus on operating energy-efficient data centres with guidelines on deployment.
PO1-B	PM4 complements the upcoming Regulation on accelerating and streamlining environmental assessments, which focuses on administrative simplification for environmental assessments, by adding a facilitator to accompany all permitting stages (incl. beyond environmental assessments) for a given data centre project. PM5 complements envisaged provisions for industrial acceleration, notably in the upcoming Industrial Accelerator Act, where areas and measures for industrial acceleration focus on manufacturing industries and do not account for the specific needs (e.g. connectivity) and benefits (e.g. their ability to provide flexibility services to the grid) of data centres, which are a services industry and thus not in scope of the Industrial Accelerator Act. PM6 steers national funding towards the deployment of innovative and sustainable data centres, while PM7 complements and ultimately leverages the existing Digital Decade monitoring cycle. The scale of the compute capacity gap and its impact on EU competitiveness require such dedicated support measures for data centre deployment, which cannot be achieved by horizontal initiatives that omit the specific needs of data centres.
PO1-C	PM8 complements existing framework programmes, which do not sufficiently cover data centre innovation and deployment. PM9 creates the possibility, without prejudice to the outcome of the negotiations on the next MFF proposal, for strategic data centre 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. PM10 is an EU-level version of PM5.
PO1-A, B, C	PO1 B and C would leverage the future rating scheme for data centres under the Energy Efficiency Directive as a way of identifying particularly sustainable data centres. Moreover, they would build on other initiatives which address data centre input factors, such as the future Grids Package (energy) or the future Digital Networks Act (connectivity).

PO	External coherence
PO2-A	PM11 would provide the first-ever definition of a sovereign cloud and AI computing service, going beyond technical cybersecurity and thus complementing the Cybersecurity Act (CSA). PM12 adds guidelines for providers and PM13 is a new way of enhancing visibility of sovereign offerings. PM14 is designed to complement the Data Act's provisions on interoperability standards by enacting flanking measures that ensure the usability of the tools created by the Data Act, notably by advancing standardisation work.
PO2-B	PM15 complements the cloud cybersecurity certification under the CSA and uses it as a way of assessing whether a service is sufficiently cybersecure. However, the focus of the sovereignty scheme is fundamentally different as it covers sovereignty in a way that is not addressed by any other initiative, including the AI Act, which is a product safety legislation. PM16 complements the horizontal procurement acquis with the necessary sectoral approach that accounts for the nuances of purchasing cloud services, i.e. services with a global value chain, and empowers public purchasers to reward specific service characteristics which the horizontal acquis cannot provide for. By focusing on cloud and AI computing services, it is clearly delineated from the AI Act, which sets safety requirements for AI systems and general-purpose AI models. PM17 creates the tools for joint procurement, so far non-existent in this sector. The same is true for PM18 which is an entirely new addition to the EU's policy toolbox.
PO2-C	PM20 is a new policy tool, with no legal precedent. PM21 makes the use of the sovereignty risk assessment under PM15 mandatory, leveraging the NIS2 Directive to identify sectors of high criticality. Beyond giving a framework for cybersecurity certification, the CSA deals with supply chain risks with a specific focus on high-risk vendors. However, it does not address public procurement. PM21 complements the CSA in that respect. This is enhanced by PM19, which mandates the use of specific award criteria for all public procurements of cloud and AI computing services, thus complementing the Procurement Directives. PM22 leverages the tools of PM17 and establishes the first-ever EU framework for joint procurement in this sector. PM23 leverages and complements the European Competitiveness Fund, while PM24 presents an entirely new policy tool.
PO2-A,B,C	All PMs under PO2 would build on the Data Act's provisions on the right to switch and use different cloud services in parallel, which is a prerequisite for users to diversify or change the cloud services they use.

Several existing and planned pieces of legislation and policy initiatives relate to the **specific objectives** pursued under this initiative. However, each of them shows **gaps with respect to reaching these objectives**, which this initiative would fill. The table below illustrates this in detail and elaborates on the relationship of these other pieces of legislation or policy initiatives with the future Cloud and AI Development Act.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
SO1 - Increase computing capacity deployed in the EU through innovative and sustainable technologies	The **Horizon Europe programme** provides funding for research and innovation in the EU, including in digital technologies. Cluster 4 (Digital, Industry and Space) covers enabling technologies like cloud as well as advanced computing.	Horizon Europe lacks scale to meaningfully advance innovation in computing capacity. Between 2021 and 2027, the total budget of Horizon Europe amounted to EUR 95.5 bn. Estimates indicate that in 2023 only, the part of AWS's R&D spending on cloud computing alone was ca. EUR 18 bn[188]. This initiative aims to ensure that innovation in computing capacity becomes a stand-alone objective. EU Framework Programmes also suffer from a gap between R&D and commercialisation. For example, the SUNFISH project[189] devoted 4.5 m of Horizon 2020 budget to developing a solution for secure information sharing in federated heterogenous private clouds. However, no European cloud provider was able to capitalise on the project outcomes, which were not widely taken up. This initiative aims to tackle not just the development but also the uptake of innovative technologies through dedicated deployment measures and incentives for the deployment of innovative data centres.
	The **IPCEI for Next Generation Cloud Infrastructure and Services** involves 19 companies from seven	The focus of this IPCEI is on research, development and innovation. Beyond that, it only covers the first industrial deployment of innovative solutions

[188] How much does Amazon invest in R&D? Here's an informed guess.
[189] SecUre iNFormation SHaring in federated heterogeneous private clouds | SUNFISH | Projekt | Fact Sheet | H2020 | CORDIS | European Commission.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	Member States: France, Germany, Hungary, Italy, the Netherlands, Poland, and Spain. These seven Member States provide up to EUR 1.2 bn in public funding to developing data processing capabilities, and software and data sharing tools that enable federated, energy-efficient and trustworthy cloud and edge distributed data processing technologies and related services.	(particularly in edge computing). Most notably, the IPCEI focuses on beyond-the-state-of-the-art solutions. Consequently, the IPCEI does not target capacity deployment in a way that would contribute to closing the current compute capacity gap. Moreover, compared with innovation efforts by leading international cloud providers, the funds available to European companies under this IPCEI are much lower. However, the research and development efforts supported under this initiative will build on and integrate achievements under the IPCEI. Moreover, deployment incentives will positively affect the broader deployment of solutions developed under the IPCEI.
	The **AI Factories** and future **AI Gigafactories** already/will provide high performance computing capacity to developers and deployers of AI models. The initiatives leverage the EuroHPC Joint Undertaking.	These initiatives mainly serve to drive advancements in AI applications across different sectors, going beyond the capabilities of general-purpose and AI-optimised data centres. They focus on large concentrations of computing power needed for the training of AI models. They do not address the deployment of more decentralised computing capacity in data centres, necessary for the large-scale uptake of AI throughout the EU and for enabling lower latency. The deployment of AI Factories and Gigafactories may benefit from measures under this initiative, such as identified areas for accelerated deployment.
	The **Energy Efficiency Directive** contains measures on improving the energy performance of data centres. It encourages waste heat re-use and requires data centres above 500 kW to report annually on their energy usage and on other sustainability metrics. This reporting will form the basis for a **future rating scheme**, which will be enacted as part of the upcoming Data Centre Package.	The Energy Efficiency Directive is the key piece of legislation for guiding the data centre industry towards greater energy efficiency through measures such as reporting and the future rating scheme. However, beyond transparency measures and reputational considerations, the Directive does not set incentives for data centre operators to improve their sustainability performance and does not contain measures for accelerating the roll-out of sustainable data centres across the EU or increasing related investment (although the possible

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	This will also kick off the work on a separate proposal for data centre minimum performance standards, building on the sustainability metrics established under the Energy Efficiency Directive.	establishment of minimum performance standards, stemming from the Directive, could set the minimum specifications of sustainability for future data centres in Europe). The initiative will contain measures to incentivise the roll-out of energy-efficient data centres. To identify which data centres are sustainable, this initiative will refer to the rating scheme developed under the Energy Efficiency Directive.
	The Regulation laying down **ecodesign requirements for servers and data storage products** sets requirements for sustainable products.	Data centre hardware is subject to minimum performance and information rules; however, the Regulation does not contain measures to directly incentivise the deployment of innovative and sustainable technologies.
	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 and measures progress in all Member States and at EU level.	Beyond the edge node target, the DDPP does not contain targets for the deployment of compute capacity or data centres in the EU. And beyond setting out targets and monitoring progress (2257 edge nodes in 2024), it does not contain concrete support measures for such deployment. This initiative will complement the DDPP in this regard: The data centre capacity target would be integrated into the DDPP, and by leveraging the existing yearly monitoring exercise, this initiative would create synergies with the DDPP.
	The **EU Code of Conduct on Data Centre Energy Efficiency** is a reference document to assist data centre operators in identifying and implementing measures to improve the energy efficiency of their data centres. This Best Practice document contains a full list	The Code of Conduct does not concern measures to deploy a data centre, instead focusing fully on practices for operating it.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	of the identified and recognised data centre energy efficiency best practices within the Code of Conduct.	
SO2 - Ensure attractive conditions for the deployment of sustainable and innovative computing capacity	European **Grids Package**, put forward by the Commission [on 10 December 2025] aims to modernise and enhance the EU's electricity grids. It contains targeted legislative changes to the TEN-E Regulation and related regulations and directives, with a view to improving pan-European grid planning. It will consider permitting for grid expansion and cost-sharing in a cross-border context, as well as providing guidance on measures to accelerate grid connections within the current legislative framework.	As discussed throughout this assessment, energy is a key input factor for data centres and sufficient grid capacity is a prerequisite for their deployment in the EU. The European Grids Package aims to ensure grids will be in place and ready to uptake future loads in a horizontal manner, as the issue at stake (lack of grids capacity) concerns more stakeholders. The initiative assessed here focuses on data centres as an ultimate client of grid capacity in the EU. It aims to complement the Grids package by ensuring data centres location considers grid availability, information is exchanged sufficiently in advance to feed into grid planning and hence ensure timely connection of data centres. The guidelines on grid interconnection lay down ways in which Member States can accelerate grid connections, including a more efficient structure of their grid connection queue, for example by considering a project's readiness and grid-friendly uses as opposed to a pure first-come-first-served approach. It also requires strong involvement of industry, including data centre sector in the grids planning. This initiative will leverage these considerations, for example by clarifying that public support for strategic projects shall only concern projects which are able to provide needed flexibility for the grid, as required by relevant technical conditions, for the sake of their efficient grid integration.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	The future **Digital Networks Act** (DNA) seeks to incentivise the building of the digital networks of the future and improve digital connectivity for end users.	The DNA will improve digital connectivity for end users and thus be beneficial to the deployment of data centres in the EU, for which high-performance connectivity is a prerequisite. This initiative will leverage the DNA's advancements for connectivity and will thus stay focused on the deployment of the data centre (where data processing occurs), not the prior or parallel build-out of the necessary connectivity infrastructure. The two initiatives are thus complementary. The DNA will also address the convergence of network infrastructure. For example, it will address scenarios where a cloud service provider operates a network and has so far not been subject to obligations under the Electronic Communications Code. The intention is to clarify the modalities of interconnection between operators of networks and other market participants. This relates to a specific market situation and is not impacted by possible measures under this initiative.
	The **Gigabit Infrastructure Act** sets rules to accelerate the rollout of Gigabit networks installations.	While data centre operators and cloud service providers will benefit from an improved rollout of very high-capacity networks, the Gigabit Infrastructure Act does not cover the constructions of data centres. This initiative would thus build on the advancements in accelerated network deployment under the Gigabit Infrastructure Act.
	The upcoming **Industrial Accelerator Act** will set rules for foreign investment contributions and create clusters of industrial activity for the manufacturing sector	On permitting, the IAA sets out the principle of 'one project, one procedure' and establishes a single digital procedure to cover the entire permit-granting process. It also puts forward other measures to accelerate permitting (time limits for project approvals, single point of contact, overriding public interest

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
		etc.). This initiative will leverage the newly created approach to simplified and digitised permitting by cross-referencing the IAA. The IAA will require Member States to designate at least one manufacturing industrial acceleration area/cluster where further business facilitation measures apply (prioritised access to materials, access to EU finance, regulatory sandboxes etc.). However, these areas won't account for the specific needs of data centres, which are a services sector. While data centres consume a lot of energy, a characteristic they share with other more traditional industries, they present several fundamental differences. First, unlike industries that may adjust energy use based on production schedules, the energy demand of data centres are more constant, as their primary purpose is to ensure continuous service and data availability. Moreover, data centres can assist the grid through flexibility services. Second, their quality-of-service obligation imply that data centres are equipped with powerful energy generation capacities that can be leveraged by grid operators for flexibility purposes. Third, unlike other energy-intensive industries, the physical location of a data centre is dictated by the presence of robust connectivity: low latency is critical for supporting the real-time data processing and application needs of other industries, such as financial transactions or AI applications. That is why the cloud and AI Development Act will complement general industrial acceleration measures with measures that are tailored to the accelerated deployment of data centres.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	The **future Regulation on accelerating and streamlining environmental assessments** will simplify and speed up environmental screenings and assessments.	Data centres are not subject to mandatory environmental impact assessments under the existing Environmental Impact Assessment Directive. However, Member States can determine themselves that an individual data centre project should undergo such an assessment, causing them to be de facto mandatory in many Member States. The new Regulation will establish a toolbox with additional provisions (overriding public interest, tacit approval and dispute settlement) that can be leveraged in sectoral legislation regarding strategic sectors or categories. For all environmental assessments, the new Regulation establishes streamlined provisions, including maximum timelines for the duration of the screening process and for decisions by competent authorities. Procedurally, the proposal sets up a single point of contact for Environmental Impact Assessment and digitises and streamlines assessment procedures (e.g. through the re-use of documents across different stages). The future Regulation on accelerating and streamlining environmental assessments focuses on environmental assessments, not on other steps of the permitting process such as zoning and land allocation and building permits. The cloud and AI Development Act will leverage these simplifications and complement them, notably by establishing a facilitator to accompany data centre operators throughout their overall permitting journey, not only the possible environmental assessment. The cloud and AI Development Act will also leverage the toolbox established by the new Regulation, by referencing it within the Act to activate the additional provisions for strategic data centre projects.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	The **Net-Zero Industry Act** (NZIA) sets out to boost the EU's manufacturing capacity for net-zero technologies, e.g. through simplified permitting and areas for faster deployment.	Data centres do not qualify as net zero technologies. The acceleration measures under this initiative are thus not in conflict with NZIA. Data centre operators may however benefit from NZIA as downstream customers or users of net zero technologies such as batteries.
	The **Renewable Energy Directive** (RED III) simplifies and accelerates permitting procedures for renewable energy and storage projects, including by establishing renewables acceleration areas.	Data centres may benefit from the increased availability of renewable energy and storage in the EU but are not themselves covered by the Directive. This initiative is thus fully complementary to RED III and can leverage it: Proximity to renewables acceleration areas may be a relevant factor in designating sites for faster data centre deployment.
SO3 - Decrease the overall reliance on non-European cloud and AI computing services	The **Data Act**, which enters into application in September 2025, enables cloud switching by removing key sources of contractual, commercial, and technical vendor lock-in. As part of this, it sets rules for fair cloud contracts, creates an EU repository for harmonized standards and open interoperability specifications, and lays the basis for standardization requests.	By enabling switching and removing key sources of vendor lock-in, the Data Act seeks to ensure that cloud service providers in the EU compete on quality, innovation, and price. It seeks to enable cloud users to freely choose the provider that best meets their needs and combine offers of different providers in a multi-cloud approach. However, the Data Act does not contain elements to shape up a more competitive offer of EU cloud services or encourage the entry into the market of a more diverse set of cloud service providers. The Data Act opens the path towards a possible reduction of dependencies on non-EU providers but does not build the road towards a more sovereign and trusted EU cloud computing sector. The cloud switching and interoperability provisions, however, make it possible for users to embrace European cloud computing services more strongly. The Data Act is thus an enabler for the cloud and AI Development Act.

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	The **Digital Markets Act** covers cloud services as a core platform service, meaning that cloud service providers designated as gatekeepers would have to comply with a set of obligations, for example related to enabling interoperability.	So far, no cloud and AI computing service provider has been designated as a gatekeeper for their services (Amazon designated for the marketplace and amazon advertising; Microsoft is designated for LinkedIn and for Windows PC Operating System). On 18 November 2025, the Commission opened three market investigations on cloud computing services under the DMA: Two market investigations will assess whether Amazon and Microsoft should be designated as gatekeepers for their cloud computing services, Amazon Web Services and Microsoft Azure, under the DMA, in other words whether they act as important gateways between businesses and consumers, despite not meeting the DMA gatekeeper thresholds for size, user number and market position. The third market investigation will assess if the DMA can effectively tackle practices that may limit competitiveness and fairness in the cloud computing sector in the EU. Irrespective of the gatekeeper designation, the DMA does not contain measures that would actively promote the uptake of sovereign cloud services. The DMA aims at remedying specific market behaviours of certain providers that are gatekeepers and thus intervenes at a different level than the cloud and AI Development Act, which focuses on the uptake and use of the services provided.
SO4 - Contribute to the protection of fundamental	The **Public Procurement Directives** cover tenders above certain thresholds and prescribe transparency, equal treatment, open competition and sound management for procurement procedures. The upcoming revision of these Directives intends to align	Public authorities in the EU rely heavily on non-EU cloud and AI computing service providers. The problem drivers justifying the policy measures of the cloud and AI Development Act regarding the public procurement of sovereign cloud and AI computing services in sectors of high criticality are very specific to the technologies and applicable legal frameworks concerned. For example,

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
interests of society by enhancing the resilience of supply of cloud and AI computing services, in particular in the public sector	them more closely with strategic goals of the EU, including resilience considerations and the announced EU preference in public procurement within strategic sectors.	a cloud computing service value chain and the underlying infrastructure used to deploy the service can be distributed across different geographies and subject to corresponding jurisdictions, including those with laws with an extraterritorial effect. Such problem drivers therefore require a nuanced and targeted sectoral approach, which is not covered by the existing Public Procurement Directives and would be difficult to account for sufficiently through an overarching EU preference approach. This initiative will therefore provide a sector-specific approach to sovereignty – the many layers of which cannot be addressed in the horizontal acquis that lays down general principles for the design of procurement procedures – which will be complemented by award criteria that are also tailored to the specificities of cloud and AI computing services.
	The **Cybersecurity Act**, currently under revision, lays down a voluntary certification framework for ICT processes, services and products – with cloud services considered as a subset of ICT services. It gives the legislative framework for adopting a European cybersecurity certification scheme for cloud services by means of an Implementing Regulation.	ENISA has been working on developing an EU-wide cybersecurity certification scheme for cloud services (EUCS), which has not yet been adopted. Certification under the CSA can address technical cybersecurity criteria but is not suited for addressing sovereignty concerns that go beyond these technical elements. This initiative will thus complement the CSA's cloud cybersecurity focus with sovereignty considerations. A finalised EUCS could be leveraged in the audit scheme for sovereign cloud and AI computing services as a way of ensuring that a service subject to a sovereignty audit meets the highest cybersecurity standards.
	The **Directive on Security of Network and Information Systems** (NIS2) sets out cybersecurity risk management and incident reporting obligations to a set	The NIS2 Directive improves the cybersecurity risk management of cloud service providers and data centres in the EU, resulting in greater trust. However, it does not contain measures geared at the uptake and use of such

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	of essential and important entities across critical sectors, including cloud services and infrastructure.	services and remains fully focused on technical cybersecurity as opposed to broader sovereignty considerations. This initiative will therefore complement the NIS2 Directive.
	The **Digital Operational Resilience Act (DORA)** aims to strengthen the digital resilience of financial entities. It ensures that banks, insurance companies, and investment firms can withstand, respond to, and recover from ICT disruptions, such as cyberattacks or system failures.	While DORA shapes compliance obligations for cloud service providers and indirectly covers AI computing service providers if they provide services to financial entities covered by DORA or if their role is significant enough in terms of operational resilience, it has a sectoral scope and is financial-sector specific. Under DORA, cloud service providers must implement ICT risk management, conduct regular testing and incident response to comply with the requirements for critical third-party service providers. The covered financial institutions, which could be public in nature, must carry out due diligence on the cloud providers they work with.
	The **Artificial Intelligence Act (AI Act)** sets out rules for AI systems and general-purpose AI models and not cloud and AI computing services. It follows a risk-based approach and provides rules to ensure that AI systems used in the EU are safe, for example by introducing safety and security requirements, such as accuracy, robustness and cybersecurity for data and data governance.	The AI Act harmonises rules for AI systems and general-purpose AI models to be placed on the EU market, improving the functioning of the internal market and promoting the uptake of human-centric and trustworthy AI along the value chain. As a product safety legislation, the AI Act ensures a high level of protection of health, safety and fundamental rights, It does not cover aspects of sovereignty regarding AI computing services, which the cloud and AI Development Act will address. The two initiatives are thus complementary.
	The **EU-US Privacy Framework (DPF)** is a mechanism established to facilitate the transfer of personal data from the EU to the US, while ensuring	While the DPF addresses transatlantic data transfers, it does not remove sovereignty concerns about dependence on US hyperscalers and on the subsequent exposure to surveillance laws, such as the US CLOUD Act,

Specific objective	Legislation or policy initiative	Gap with regards to specific objective / relationship with the cloud and AI Development Act ("this initiative")
	adequate levels of data protection. It replaces various legal frameworks that were invalidated by the EU courts for insufficient protection of personal data (e.g., the Privacy Shield). On 10 July 2023, the Commission issued an adequacy decision recognizing that US organizations certified under the framework offer an adequate level of protection so that data transfers could take place without additional legal barriers. On 3 September 2025, the General Court of the EU dismissed an annulment action, confirming that the framework is valid.	obliging US providers to hand over data to US authorities even if stored in the EEA. Moreover, the notion of sovereignty goes beyond data transfers and also relates to operational autonomy, an aspect that goes beyond the DPF. This initiative thus complements the DPF.

ANNEX 8: KEY TECHNICAL CONCEPTS

A **data centre** provides the walls, cooling, and connectivity needed to run the IT equipment that enables computing, which are typically processors mounted on servers, storage units sometimes called memory, and networking equipment. Data centre capacity is measured in megawatts (MW), indicating the total electrical power made available to the IT equipment[190]. The capacity of the equipment is therefore limited by the electrical power available in the data centre. Throughout this report, the term ‘computing capacity’ is thus used interchangeably with data centre capacity.

The International Standardization Organization (ISO) defines **cloud computing** as a “paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand”. These resources are located in data centres. Operating a data centre and providing a cloud service are two distinct segments of a same supply chain. Data centres can be owned by cloud service providers (CSPs) themselves (vertical integration). Otherwise, data centres operators are often specialised independent businesses, which rent out space for customers, including CSPs, to place their equipment in. The data centre can have a single client or multiple, which are referred to as **co-location data centre providers**. Companies which provide cloud services on a very large scale are commonly referred to as hyperscalers, a category understood to include Microsoft, Amazon and Google. For very fast response times, i.e. low latency, data must be stored and processed closer to the user, in **edge data centres** or **edge nodes**, which can be seen as mini-data centres (an edge facility can be as small as the size of a fridge, while the largest data centres can be as big as several football fields).

While data centres powering traditional cloud services and AI computing services look similar, they present important differences. First, at the microprocessor level: while data centres specialised in AI computing services use a mix of **Graphic-Processing-Units (GPUs)** and **Central-Processing-Units (CPUs)**, others are exclusively powered by CPUs. Second, GPU-powered data centres, sometimes called ‘AI data centres’, are much more energy-intensive and require a different physical layout implying a design choice from the outset, making refits difficult. Throughout this assessment, the term ‘data centre’ is used to refer to both types of data centres in order to be future-proof and end-use agnostic.

[190] This is a widespread industry practice. However, it is imperfect as it does not reveal the type, quantity and capacity of the chips hosted in the data centre and does consider the efficiency of this equipment.

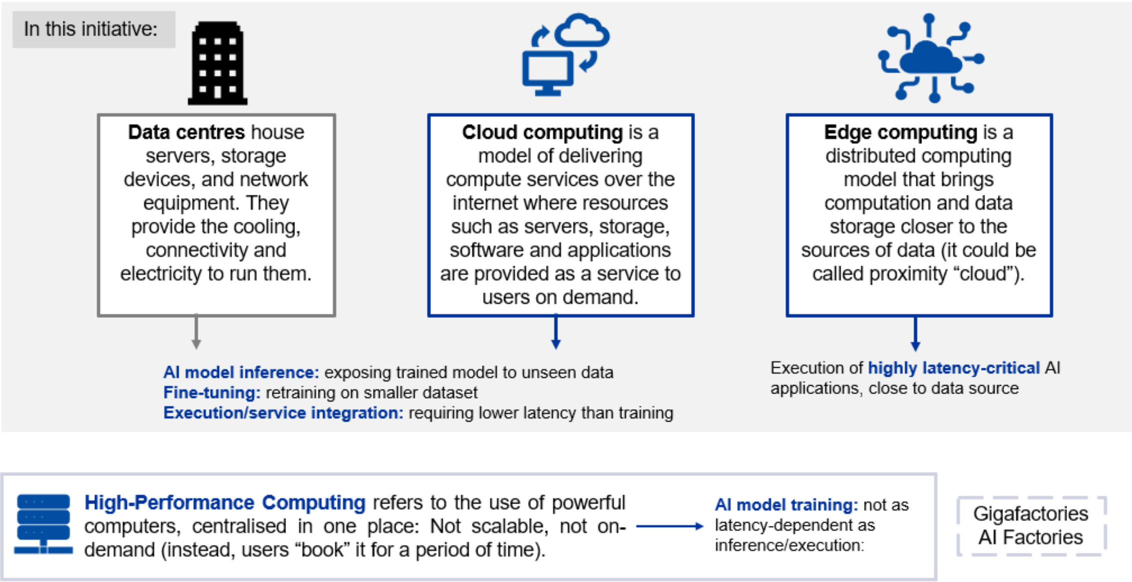


Figure 1. Key concepts along the cloud and AI value chain

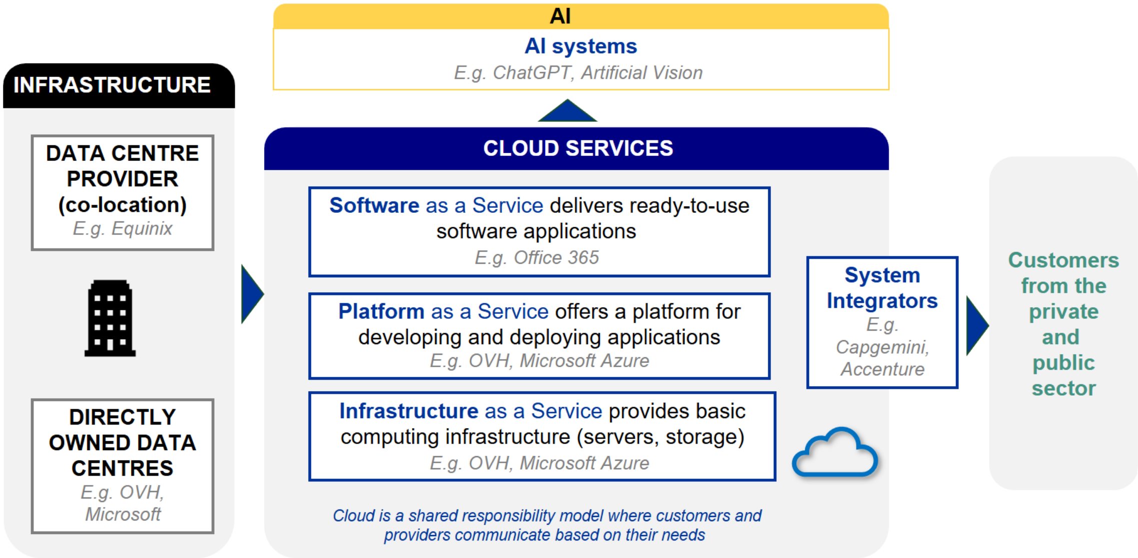
When **training an AI model**, longer response times/higher latency are not as problematic while a large concentration of computing power is paramount. The size and complexity of an AI model is often described by the number of parameters it is built on, a figure that can reach a trillion. Training a model, even on the worlds' largest computing facilities, can take several months of uninterrupted calculation. That is why training is usually executed in **High-Performance Computing** (HPC). HPC is provided over specialised data centres and differ from cloud computing in the sense that, typically, the pool of resources is not shared and/or not scalable and/or not elastic. Conversely, the **fine-tuning, inference** and service integration of AI models rely on cloud or even edge computing. Fine-tuning an AI model consists in customizing pre-trained models using domain-specific data. Inference then uses this fine-tuned model to generate predictions or outputs on new, unseen data by applying the learned parameters without further training. Edge computing makes it possible to run AI applications close to the data source, allowing for very low latency, for example in AI-assisted real-time imaging and surgery, in autonomous navigation and real-time decision-making in autonomous driving. The different stages of an AI model, reaching from training to application, including with low response times, require a continuum of computing capacity spanning HPC, data centres, and edge nodes.

Cloud services are often broken down in three layers: infrastructure-as-a-service (IaaS) consists in supplying basic computing services, essentially storage and raw processing; platform-as-a-service (PaaS) consists in offering a platform over which services can deployed; and software-as-a-service (SaaS) is a software application delivered over the cloud such as an office automation suite or a video streaming service. Cloud service providers can offer services that span across all layers (e.g. Microsoft offers Office 365 running over its own Azure infrastructure), or not (e.g. Netflix operates over Amazon's infrastructure). Cloud computing and **AI** are deeply interconnected, each fuelling the other's potential. Cloud computing provide the scalable infrastructure and computational power AI needs to process data, train models, and deploy applications efficiently. In turn, AI enhances cloud services through automation, predictive analytics, and smarter resource management, making them more adaptive and user-friendly. AI computing services provide computing infrastructure that allows users to run trained AI model (inference) without hosting the AI system on their own hardware. Moreover, AI functionalities are increasingly integrated into cloud services, for example into SaaS offerings, to enhance their functionalities.

This assessment systematically uses the term 'cloud and AI computing services' understood as offering computing resources for the running (inference) of AI systems. AI systems, pursuant to the AI Act, are not covered by the sovereignty scheme described in this Impact Assessment.

Cloud services may also include other data processing-related services, e.g. data analytics[191].

Figure 6. Interplay between cloud and AI



[191] The Digital Decade Policy Programme, for example, measures uptake for AI, cloud and big data together: ['Path to the Digital Decade': the EU's plan to achieve a digital Europe by 2030 - Consilium].

ANNEX 9. BASELINE SCENARIO (POLICY OPTION 0)

The baseline scenario represents the reference case against which policy options are assessed. It provides a realistic and neutral projection of how the EU cloud and AI computing services market, and the related data centre infrastructure, are expected to evolve in the absence of additional policy intervention beyond current measures and commitments. The scenario integrates the effects of:

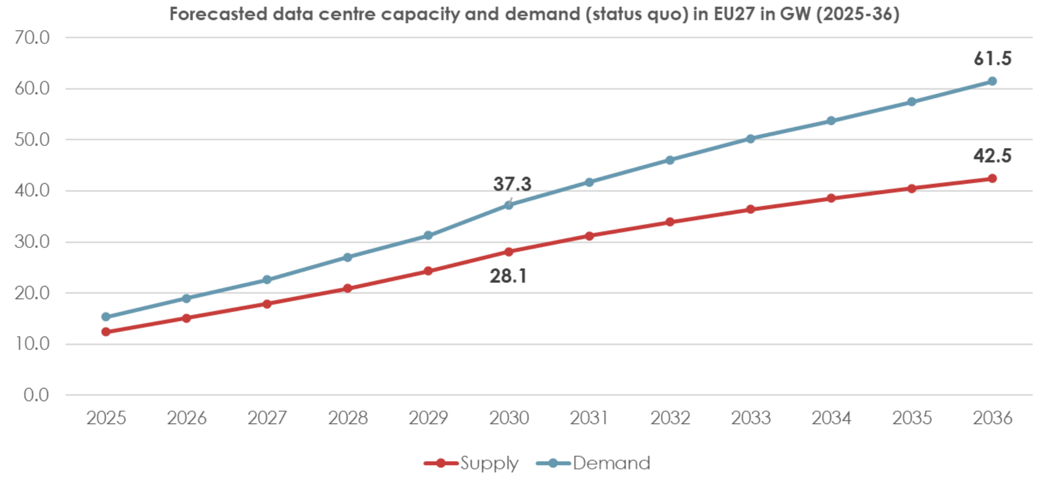
- Existing EU legislation, especially for infrastructure development (EED and RED III), that is Problem 1. In the case of cloud services (Problem 2), the main applicable legislation is the Data Act, which entered into force in September 2025, whose effects are not yet observable. Similarly, the impact of EU public funding cannot yet be fully assessed, as the current Multiannual Financial Framework (MFF) is still subject to evaluation. In addition, no dynamic outlook on future funding allocations can be provided, given that negotiation on the next MFF have not yet started;
- Market-driven technological progress and private investment trends;
- Macroeconomic forecasts;
- Global developments affecting demand for computing capacity, cloud services, and AI workloads.

It covers the period 2025-2036 and the EU-27, compares to global market evolution and provides a projection of likely developments in the absence of further policy action, thus allowing for the quantitative and qualitative comparison of the policy options' expected impacts. It describes how each identified problem and their underlying drivers would develop to 2036 without new policy action, drawing on available quantitative evidence and market projections.

1. Limited and geographically concentrated availability of computing capacity

For problem 1, The EU's total installed compute capacity, measured in data-centre IT load, stands at approximately 12.4 GW (and 13.9 GW if public sector capacity is also considered), representing around 20% of global capacity. Growth is projected to reach 42.5 GW by 2036, yet in the central scenario demand data centre capacity is expected to increase to 61.5 GW over the same period, creating a structural capacity gap of 19 GW relative to projected needs, as shown in the figure below.

Figure 7. Forecasted data centre capacity and demand in EU-27 (Source: Technopolis et al. (2025))



In this central scenario data centre demand growth is based on the following assumptions:

- Enterprise IT budgets across the EU-27 continue to expand at a steady and predictable pace, reflecting a stable macroeconomic environment and a measured approach to digital transformation.
- IT spending as a share of enterprise turnover increases gradually, reaching 3.7% by 2032. From 2032 onwards, this ratio stabilises, indicating a maturing digital spending profile with spending only increasing to 3.8% by 2036. Within this broader trend, investment in data centre infrastructure grows in line with the historical CAGR of 14% through to 2030, reflecting sustained demand for compute and storage infrastructure. This growth supports both the retrofitting of legacy environments and the deployment of new, AI-capable facilities, particularly in markets where cloud adoption and enterprise workloads continue to scale. From 2032 onwards, the growth rate of data centre spending decelerates, but outlays continue to increase, sustained by lifecycle refreshes, AI-capable retrofits, compliance and resilience upgrades, and steady colocation demand
- Workloads evolve steadily, with increased deployment of AI, machine learning, and data-driven services contributing to higher computational requirements.
- Digital policies boost private sector demand. As governments roll out e-government services, data-sharing initiatives, and sector-specific AI guidelines, private enterprises respond by adopting initiatives which steadily drive increases in compute and storage requirements.

Data centre supply growth is based on the following assumptions:

- Capacity growth is around 14% CAGR through 2025–2030, then eases over 2030–2036.
- Expansion remains concentrated in FLAP-D hubs, with steady investment in secondary markets (Nordics, Spain, Italy) and slower uptake in developing markets (around 6.49% CAGR). Capacity expansion follows market trends concentrated in existing hubs, where grid constraints, land availability, and permitting delays limit new deployment. Investment remains market-led; new entrants face high upfront capital costs (around EUR 8-10 million/MW).
- Aggregate growth is around 17.7% over 2025–2030 (consistent with the survey's ~14% CAGR lens) as committed pipelines, AI-readiness upgrades, and new cloud regions come through. From 2031–2036, growth moderates to around 7.1%, reflecting tighter site selection driven by power and land availability, longer permitting lead times, and higher financing costs. This trend risks constraining AI model training and cloud workloads within the EU, particularly for SMEs and public-sector users.
- Electrical grid limitations remain a key issue in certain primary markets such as Ireland and the Netherlands. However, regulators and operators in several markets have begun investing in grid modernisation and demand management. Without targeted policy intervention long lead times for grid connection remain across Europe (>30 months).
- The Energy Efficiency Directive requires operators of large data centres to disclose annual energy and water use, improving transparency and benchmarking. Efficiency improvements are moderate, but do not offset the growth in total electricity demand, which is expected to rise from 105 TWh to over 200TWh in 2036. Energy consumption by data centres could reach around 340 TWh annually in 2036, growing at a compound annual growth rate of 11.4%. If electricity production remained stable at the levels

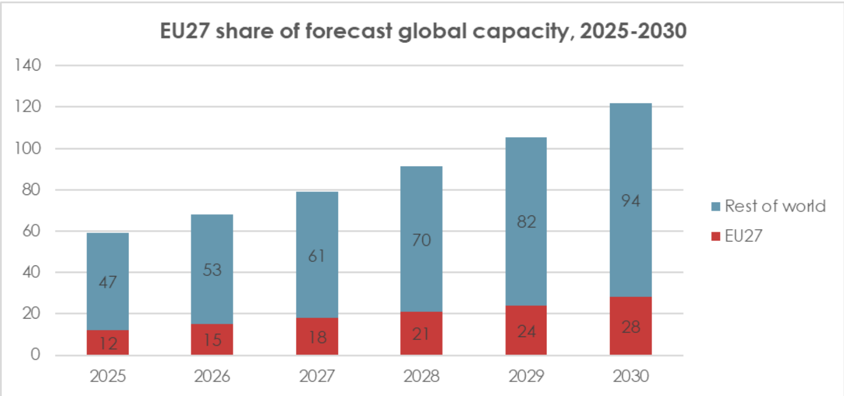
reported by the IEA in 2022 then data centres would consume 12% of EU27's generated electricity.

- Energy efficiency in data centres improves gradually; the average Power Usage Effectiveness (PUE) declines from 1.29 in 2025 to about 1.23 by 2036.The carbon intensity of this demand declines as the electricity mix decarbonises under the *Fit for 55* package. Incremental advances in cooling, waste-heat recovery, and on-site renewable generation occur as a result of existing regulatory incentives under EED and RED III.
- Surveys have identified permitting delays (up to 3-5 years in some jurisdictions), grid-connection queues, and land-use restrictions as principal d availabili new capacity. Without policy harmonisation, these bottlenecks persist, with moderate alleviation from national administrative reforms. Therefore, data centre expansion continues but below potential. Under continued existing conditions, roughly 25-30 % of announced projects experience significant delay or downsizing
- Governments aim to balance digital infrastructure expansion with environmental priorities by introducing power efficiency targets, and sustainability requirements. National measures, such as tax incentives for green data centres in the Nordics or Italy's simplified permitting for renewable-powered facilities, continue at present scale
- Policy evolution remains gradual and inconsistent, creating a fragmented regulatory landscape across Europe. Efforts to modernise infrastructure and streamline permitting are underway, but progress is uneven, often slowed by regulatory complexity and localised decision-making.

Under policy option 0, Europe's compute supply increases in absolute terms but lags behind global competitors. North America and Asia-Pacific expand faster, increasing their share of global compute. The EU maintains its global market share of around 20-23%. While the region remains attractive for investment due to regulatory stability and skilled labour, its relative cost position remains less favourable than that of North America or some Asian economies. Considering the sectors and region's expected growth and technological developments in AI, quantum computing and 6G, international providers are expected to maintain a strong EU presence under existing trade and competition rules.

Goldman Sachs forecast that total global capacity will reach 122GW by 2030, growing at a CAGR of 16%. The forecast produced by the study indicates that EU27 capacity will grow at 18% over the same period, meaning EU27's share of data centre capacity is expected to grow from 20% (2025) to 23% (2030), as shown in the figure below.

Figure 8. EU-27 share of forecast compared to the global capacity (Source: Technopolis et al. (2025))



Estimates for the United States suggest that by 2028 data centres will account for between 7-12% of total consumption.[192] The IEA in turn estimate that data centre electricity consumption in the United States will grow to 240 TWh annually by 2030 (from 180 TWh in 2024). This would equate to 6% of the United States' 2024 electricity consumption. The IEA also estimated China's data centre electricity consumption to grow to 175TWh (from 100 TWh in 2024). This would equate to 2% of China's 2024 electricity consumption.[193]

2. Dependence on cloud and AI computing services supplied by non-European providers

For problem 2, the baseline scenario describes how the market share of European providers evolves without any EU intervention beyond initiatives and regulations already adopted, such as the Data Act.

The core aim of the Data Act is to reduce friction when switching from cloud provider, but its full effects will take time to materialise.

Since October 2025, a set of standard contractual clauses recommended by the Commission will make contractually easier for cloud users to switch from provider, as they are progressively adopted. Also, by January 2027, switching from one cloud provider to another should be free of charge. Finally, aspects related to the technical switching will take more time to fully materialise. A soon to-be-published Commission study has identified only a handful of industry driven specifications that the Commission will propose to become mandatory through the foreseen mechanisms of the Data Act. This will require the adoption of several implementing acts following which industry will have a 12-month transition period to ensure compatibility of relevant data processing services with the specifications. Further standardisation will have to undergo a formal request from the Commission to the European Standardisation Organisations, a process prone to take time.

The effects of the Data Act for facilitating the emergence of an integrated offering by European providers are at this stage therefore limited and indirect. Finally, it must be noted that switching is a customer-driven operation and the effects on European providers and the growth of their customer base rely on the willingness of customers to make use of their new right to switch

The baseline presented for the policy scenario 0 for problem 2 is dynamic and focuses mainly on IaaS and PaaS using data from Synergy[194] on the market share (15%) and Statista for the market revenues (EUR 125.22 bn)[195]. Due to the heterogeneity of the SaaS market and the unclear categorization of what is included in the SaaS category, these are excluded from the baseline scenario. AI computing services can be considered as an extension of cloud services for the specific purpose of running an AI model. The two categories overlap significantly, and AI computing services are currently not separately

[192] Berkley Lab (2024). 2024 United States Data Center Energy Usage Report. Available at: https://escholarship.org/uc/item/32d6m0d1
[193] IEA (2025). Energy and AI. Available at: https://www.iea.org/reports/energy-and-ai
[194] Synergy Research. Data from July 2025.
[195] Statista

captured in statistics. That is why the below considerations are based entirely on figures and developments related to the above-mentioned market for cloud computing services.

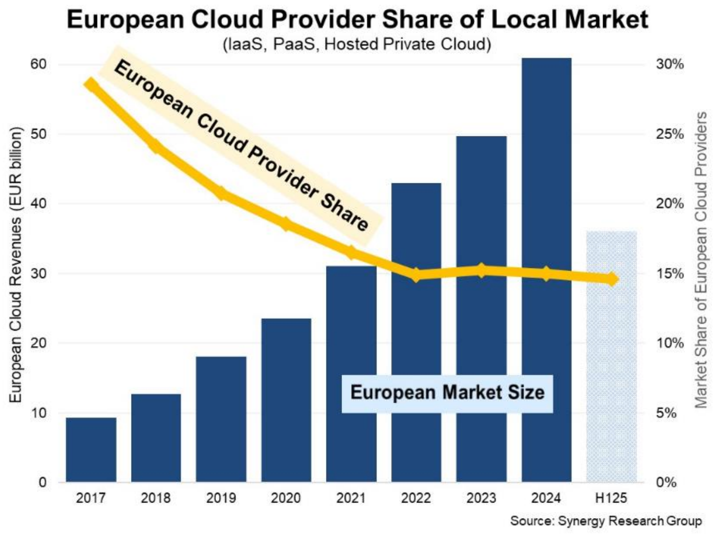
The base year considered for the baseline scenario is the latest full year for which there is stable data available, namely, 2024. In this base year, Synergy shows that EU-headquartered providers account for around 15% of the EU cloud infrastructure market, with the remainder provided by non-EU firms, in particular large US and other global providers. The base-year distribution and levels are taken as factual anchors. The dynamic baseline is built around the following assumptions:

- The European cloud market grows at CAGR 17% until 2030, as pointed out by Synergy and from 2031 to 2036, it is assumed to grow at a slower CAGR of 12%.
- Within the EU market, the market share served by EU providers, follows a flat scenario until 2036, similar to the almost flat trend that can be observed in the last two years. This is the status quo scenario.
- Two sensitivity variants are also considered:
    - A declining scenario, falling from the current market share of 15% to 10%. This is the pessimistic scenario.
    - A slightly optimistic scenario, rising from the current 15% to 17%.

The time horizon for the baseline spans until 2036, which is the time used for the modelling of the different policy measures, and a reasonable period in which structural changes in the dynamics of the cloud market can be expected.

In terms of market volume, the assumption is that, while the market grows, the EU providers' market share grows in parallel, but it slightly loses weight in the total market, leading to a small decline in European providers 'overall share of the cloud market revenues.

Figure 9. Market share of European cloud providers in the European market (Source: Synergy Research)



Within the evolving European cloud market, the central dynamic baseline assumes that EU-headquartered cloud service providers are unable to fully keep pace with their non-EU competitors. Due to a growing demand in the EU, the revenues of the European players keep steady, but their overall position barely holds.

These projections are grounded in recent market evidence (see Figure 9) and structural factors. Over the last years, European cloud providers' local market share has declined from roughly 29% in 2017 to about 15% and has since stagnated at that level, despite continued strong growth of their absolute revenues, as it can be seen in the figure above. At the same time, the three leading hyperscalers invest at a scale (around EUR 10 bn per quarter in European CAPEX according to Synergy research[196]), which results in very high barriers to significantly increase the market share for smaller European players. This suggests that in the absence of major policy interventions or market shocks, the relative position of EU providers is likely to remain broadly unchanged in the mid-term. The only cloud – specific policy currently applicable in the EU, the Data Act, entered into force in September 2025. As explained previously, its effects are not yet observable, rendering difficult to provide a more dynamic outlook than the one shown here.

The 15% used as the baseline reflects steady but constrained growth driven by potential gradual demand shifts generated by rising sovereignty expectations and niche market needs, while still facing structural issues (e.g. lock-in to hyperscalers, bundling advantages and integration needs). The 10% pessimistic scenario assumes that there is a widening AI infrastructure investment gap between US and EU cloud and AI service providers combined with regulatory initiatives failing to deliver meaningful constraints on lock-in, dampening switching and interoperability, along with price pressure from bundled offers and potential providers exits triggering a collapse in customer confidence towards cloud. The more optimistic scenario, 17%, assumes improved interoperability and portability and more trusted EU-level assurance, raising conversion rates and accelerating adoption.

All three scenarios converge within a narrow seven–percentage-point band because the core competitive disadvantages faced by European cloud providers are deeply rooted. Even in the most optimistic case, European providers only recover to about 17% market share. This is largely due to Europe's fragmented regulatory environment and the difficulty of scaling cloud and AI services, that can match the breadth and integration of those offered by the hyperscalers. Conversely, the 10% pessimistic scenario includes the demand of cloud and AI services by highly regulated sectors that are genuinely sovereign. These needs ensure a stable baseline level of demand of cloud services.

Other considerations taken into account for the assumptions include structural market factors, demand-side dynamics and competition environment, as described in section 2, notably 2.2.

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

Considered together, the three presented trajectories present a dynamic baseline scenario (Policy Option 0) towards which the EU cloud market is likely to continue evolving if the

[196] https://www.mobileeurope.co.uk/european-cloud-providers-tread-water-in-growing-market/

EU will not adopt any additional policy measures. Under this scenario, the global and European cloud markets would modestly grow but without a strong quantitative shift in the structure. This would lead the EU to remain structurally dependent of non-EU players covering most customers' needs. Furthermore, EU-homegrown providers' scale and investment in capacity and creation of new services would remain limited, constraining their ability to compete, especially with hyperscalers that present a more integrated and wider offer. In the absence of an EU action, European providers won't meaningfully improve their positioning in the market and European cloud users will continue to rely heavily on non-European providers.

Policy options under PO2 are measured both in quantitative and qualitative terms. Quantitatively, policy options are evaluated by how much they shift the baseline trajectory in terms of higher market share of European providers and reduced dependency, especially important in highly critical use cases. Qualitatively, the baseline underlines that without an EU intervention the EU market landscape would remain characterised by a high external dependency, limited European scale and persistent asymmetries.

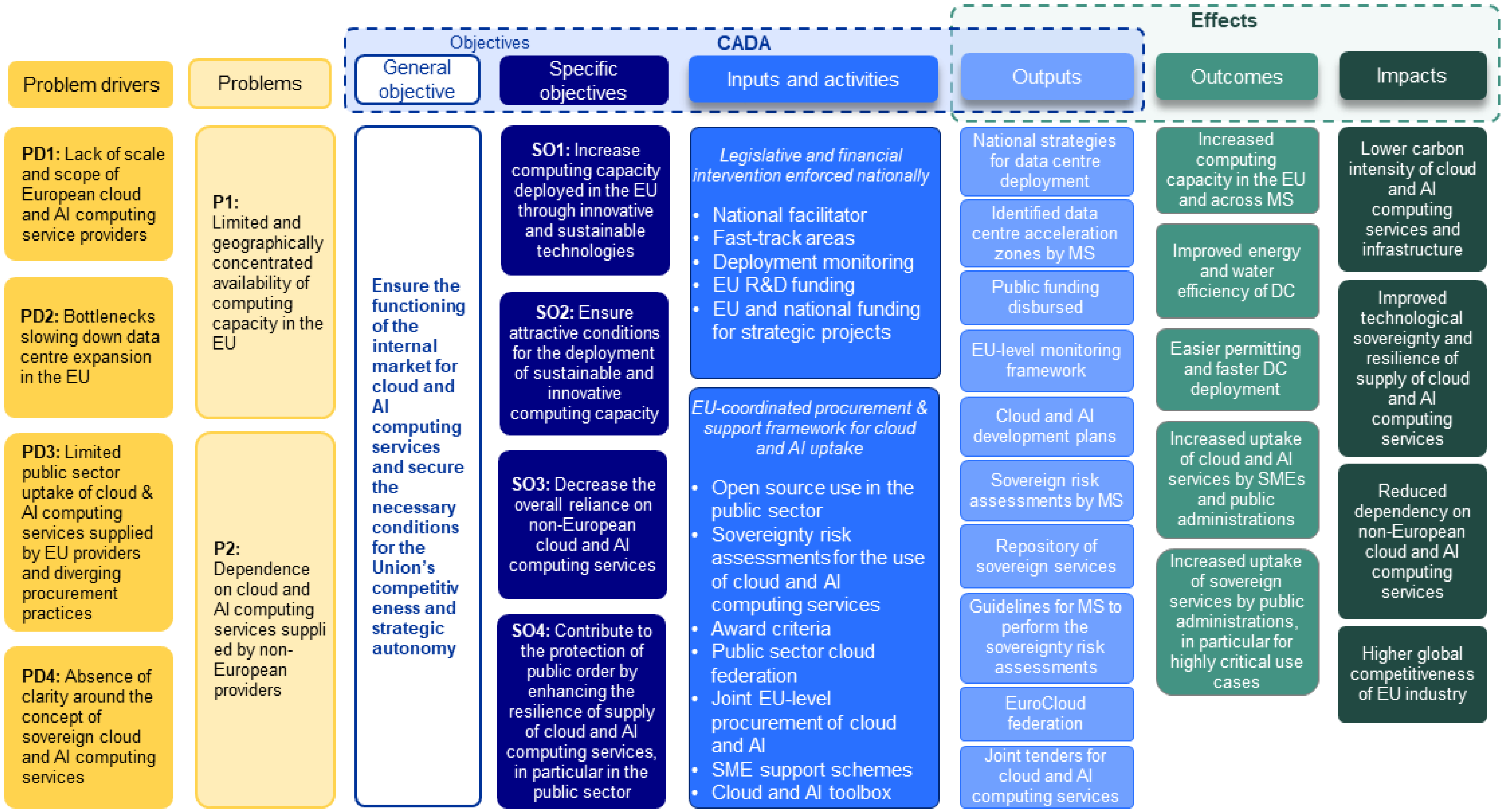
These projections serve as the counterfactual reference for quantifying the incremental effects of policy options in terms of infrastructure deployment, environmental impact, and digital sovereignty. The evolution of these challenges under the baseline scenario illustrates why EU-level action may be warranted. The objectives of the intervention, as defined in the problem tree, relate directly to the outcomes described above:

Table 69. Link between Policy Option 0 and the intervention

Problem Driver	Problem	Policy Option 0 (baseline trend)	Link to Intervention Objectives
PD1: Lack of scale and scope of European cloud and AI computing service providers PD2: Bottlenecks to expand data centre capacity in the EU	P1: Limited and geographically concentrated availability of computing capacity in the EU	• Supply grows but is outpaced by demand for compute • EU share of global compute declines. • Average project lead time ≥ 3 years; grid and permitting delays persist. • Enterprise AI use rises to 40 %, below Digital Decade target (75 % cloud, 75 % AI use in enterprises).	"*SO1: Increase computing capacity in the EU through innovative and sustainable technologies*": an increase in capacity is foreseen with a 9% CAGR. However, the industry's demand for energy will continue to grow. Without strategic energy planning and a focus on sustainable infrastructures, data centre expansion will challenge existing data centre 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. "*SO2: Ensure attractive conditions for the deployment of sustainable and innovative computing capacity*": This goal will not be met consistently throughout the EU, with geographical imbalances and potential price increases across regions.
PD3: Limited public sector uptake of cloud and AI	P2: Dependence on cloud and AI computing	• Market share of non-EU cloud providers remains 75-80%.	*SO3: Decrease the overall reliance on non-European cloud and AI computing services:* Without incentives for European providers to

Problem Driver	Problem	Policy Option 0 (baseline trend)	Link to Intervention Objectives
computing services supplied by European providers PD4: Absence of clarity around the concept of sovereign cloud and AI computing services	services supplied by non-European providers	• Cloud use in public services remain • Fragmented definitions persist; sovereignty and limited interoperability.	grow in their integrated offers as well as in the demand by main drivers of the economy such as the public sector, the dependency from non-EU providers would increase or remain the same in a positive scenario. *SO4: Contribute to the protection of fundamental interests of society by enhancing the resilience of supply of cloud and AI computing services, in particular in the public sector:* Sovereign-washing would be likely to happen without a clear definition of sovereign cloud and AI computing services and the associated enforcement mechanisms.

ANNEX 10. CADA INTERVENTION LOGIC



ANNEX 11. OPERATIONAL MONITORING AND EVALUATION SYSTEM

The monitoring and evaluation framework has been designed as an integrated system that follows each level of the intervention logic, from outputs to outcomes and long-term impact, based on a coherent set of indicators and baseline values with targets, where available. The monitoring activities will be coordinated at EU level, with the European Commission (EC, DG CONNECT) acting as the coordinator, with the support of relevant EU agencies and Member State authorities for possible data provision. The framework is defined to assess the indicators throughout the lifetime of the intervention and remain coherent with the five-year evaluation horizon.

Below are individual sections that describe how outputs, outcomes and impacts will be tracked over time, based on a coherent set of indicators for each level of the intervention logic (see Annex 10), accompanied with baseline values and targets. Each table presents data sources, collection method, frequency of collection and the responsible entity for each data input.

The underlying assumption of this approach is that digital policies produce effects through various, interrelated channels, i.e. from investment, regulation, energy systems, infrastructure, market dynamics and user behaviour, and over different time horizons. As such, the monitoring and evaluation process is to be intended not only as a tool to understand if the policy objectives have been met but also as a learning mechanism to better inform future policy implementation.

1. Output monitoring: deliverables and direct effects

At the output level, monitoring focuses on the direct and immediate results of the intervention, i.e. how the tools produced by the Cloud and AI Development Act have an immediate effect on processes and procurement dynamics. These outputs can be tracked using administrative data and information reported by operators and Member States, typically quarterly and at the end of the first year/18 months after implementation. Their goal is to ensure that the intervention is proceeding according to plan, and offer early warning on possible bottlenecks, which may need corrective measures during the implementation phase.

Indicator	Baseline	Target	Data source	Collection method	Frequency	Responsible entity
No. of national strategies for data centre and AI infrastructure deployment	<10 (out of 27 MS)	>20 (out of 27 MS)	National authorities/ Ministries' websites	Desk research	Annual	EC with MS validation (if needed)
No. of identified DC fast-track areas	63[197]	>5 per MS in the first year of	National authorities/ Ministries'	Desk research	Annual	EC with MS validation

[197] The **French** government has published a list of sites judged favourable for data-centre implantation to help attract infrastructure investment and compete at the European level. See here: 25112025__Guide Datacenters.pdf; The **German** government is developing a national strategy to promote the operation and settlement of data centres: National Data Centre Strategy - Federal Ministry for Digital and State Modernisation; Similar, **Italy** has developed a strategy for attracting investment in data centres. See: ATTRAZIONE_DEI_DATA_CENTER_2025.pdf. **Portugal** is finalising its strategy: Governo anuncia estratégia nacional de centros de dados para alimentar procura por Inteligência Artificial -

Indicator	Baseline	Target	Data source	Collection method	Frequency	Responsible entity
		implementation				
Public funding instruments operational for energy-efficient technologies/ strategic projects	NA	Definition of calls with clear eligibility rules and selection criteria	Internal	NA	Annual/ every two years	EC
Monitoring framework for monitoring data centre capacity	NA	Defined methodolog, reporting templates	Existing methodology and industry datasets	Survey + desk research + interviews	Once, to implement PM7	EC
Cloud and AI development plans	NA	>20 (out of 27 MS)	National authorities/ Ministries' websites	Desk research	Annual	EC with MS validation (if needed)
Compliance rate with the sovereignty scheme by contracting authorities	NA	Risk assessments and guidance consistently applied in major public tenders	TED data, national authorities data	Desk research + interviews with MS representatives	Annual, 1 year/ 18 months after implementation	EC with MS validation
Number of sovereign services within the repository	NA		Repository data	NA	Annual	EC
Joint tenders/procurement mechanisms launched	None	Functioning joint calls / tenders	TED data, national authorities data	Desk research + interviews with MS representatives	Annual, 1 year/ 18 months after implementation	EC with MS validation
EuroCloud platform establishment	NA	Functional platform within 1-2 years	NA	NA	Annual, 1 year/ 18 months after implementation	EC
No. of public sector open source solutions released	NA	Continuous increase	OSS catalogue	Desk research	Annual	EC

2. Outcome monitoring: mid-term change

Outcome monitoring assesses the medium-term impact of the intervention on market dynamics, user behaviours and overall ecosystem. Related indicators can be measures

---

Expresso; **Netherlands** has developed a roadmap for the growth of data centres in the country (2019): Opmaak 1; **Finland** has recently developed a national roadmap for data centres. See: National Roadmap for Data Centres : Rapporteur's Report; Spain also developed a national strategy for IA, with measures on the deployment of data centres. See: Estrategia Inteligencia Artificial 2024 through market data, structured surveys, procurement records etc. Data collection could correspond to the evaluation phase of the intervention. The monitoring framework is designed to identify key data and ensure that this is collected from a wide range of stakeholders affected by the policy intervention.

Indicator	Baseline	Target	Data source	Collection method	Frequency	Responsible entity
Installed computing capacity in the EU (IT load) and across MS (outside existing hubs)	12 GW	Additional operational IT load and AI infrastructure by 2030	Industry market studies and datasets (EUDCA, DataCentre Map)	Desk research + survey (see methodology above)	Annual and interim snapshot, 5 years after implementation	EC with MS validation
Share of EU global computing capacity	20%	≥ 25%	Industry datasets, market research	Desk research	Same as above	EC
No. of MS with simplified frameworks (permitting, zoning, energy access)	<5	≥ 20 by 2030	National authorities	Desk research + interviews	Biennial	EC
Average permitting time for new DC projects	Average time: 32 months	<18 months by 2030 and/or reduction across MS	National authorities, data centre operators, real estate analysts	Desk/market research + interviews + surveys	Annual	EC with MS validation
No. of pilot projects for innovative/ energy-efficient DC technologies	NA	Continuous increase	Project registries and evaluation	Desk research + Survey + interviews	Annual	EC
Annual public and private investment in EU DC	NA	Increase to close the capacity gap	Market analyses	Desk research + market research	Annual	EC
Improved energy and water efficiency of deployed capacity	PUE, WUE, utilisation levels today (see Annex 4)	Convergence towards best-available performance; Share of supported sites using specified cooling/power technologies	TSOs/ DSOs data, providers data	Desk research + Survey + interviews	Annual	EC with MS validation

Indicator	Baseline	Target	Data source	Collection method	Frequency	Responsible entity
Share of renewable energy used by data centres	NA	Convergence towards best-available performance	TSOs/ DSOs data, providers data	Desk research + Survey + interviews	Annual	EC with MS validation
No. of audited sovereign cloud and AI services	0	Continuous increase	Repository	Administrative data	Annual	EC
Market share of EU providers	15%	Increase in market share	Market data	Desk research	Annual	EC
Annual value of EU procurement of sovereign cloud and AI computing services	0	≥ 100%	TED data, national authorities data, audited service repository	MS reporting obligations + Desk research + interviews with MS representatives	Annual	EC with MS validation

3. Impact monitoring: long-term structural effects

Impacts concern the long-term changes, i.e. materialised over longer horizons (often beyond 5 years) in the EU's economic, technological and strategic position, following this policy intervention. Since these effects are expected to emerge progressively, they cannot be assessed through monitoring alone but should be the outcome of a more thorough analytical exercises which is able to disentangle the effects of the intervention from other policy choices or natural market developments.

Indicator	Baseline	Target	Data source	Collection method	Frequency	Responsible entity
EU computing capacity covering EU demand	2025 Gap: 3 GW	Future residual gap < 0.5 GW	Operator disclosures; ENTSO-E grid connection data; industry market studies	Desk research + survey (see methodology above)	Annual (Year-5 interim evaluation synthesis)	EC with MS validation
Lower carbon intensity of digital infrastructure	Estimated $kgCO_2e$ per compute unit (see Annex 4)	Decreasing $kgCO_2e$ per compute unit	Operator energy reporting; national grid emission factors; life-cycle assessment parameters	Desk/ market research + Survey + interviews	Annual (full assessment at Year 5)	EC with MS validation

Indicator	Baseline	Target	Data source	Collection method	Frequency	Responsible entity
Market contestability and higher global competitiveness of EU industry	Low	More bidders, lower lock-in signals, higher market shares for EU providers	Public procurement databases (TED), portability metrics from providers	Tender analytics + interviews with providers and users + survey (e.g. SME target)	At least 5 years after implementation	EC/others
Improved strategic autonomy and reduced dependencies	Baseline study	Structural reduction in dependency	Market sizing; customs statistics; provider data	Desk research	Annual + Year 5	EC/others + MS and relevant agencies

4. Evaluation arrangements and timing

The evaluation will be structured to understand how the observed impact and changes can be attributed to this specific policy intervention. The study conducted as part of the monitoring of capacity deployment during the first year of implementation will be used to validate indicators, data sources and targets. A mid-term evaluation can be conducted after the third year of implementation of the intervention, to better understand the early outcomes and effectiveness of the intervention (using data collected above). The full evaluation is then expected five years after the implementation of the intervention to assess the outcomes and identify early impacts.

To prevent parallel reporting, avoid duplication and benefit from synergies with existing initiatives, the programme should reuse:

- Eurostat business statistics
- National regulatory authorities and BEREC reporting
- Procurement electronic databases, e.g. TED
- Energy systems data from TSOs and DSOs, national energy agencies
- Existing and future programmes, such as the Digital Decade Policy Programme, RRF reporting templates

A preliminary set of evaluation questions can be found below. This will be updates and enriched following the implementation of the initiative.

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*

Evaluation criterion	Assessment objective and possible evaluation questions
	around the concept of sovereign cloud and AI computing services? How did it improve the market share of homegrown EU cloud and AI computing service operators? What is their market share? 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?*
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 12. COSTS OF MIGRATING AND PORTING APPLICATIONS

Cloud **porting** consists in moving a service from one cloud provider to another cloud provider Cloud **migrating** consists in moving a service from on-premises to cloud

Today, *by and large critical use cases* [of the public sector] *are not in the cloud*. Most of these use cases are instead run 'on-premises', that is, on local infrastructure which are not scalable (and cannot therefore be called 'cloud'). Policy measure 21 creates an obligation for the public sector to carry at least one sovereignty risk assessment to identify which public sector use cases within a Member State require the use of which sovereignty level as described under PM11. The details of the measure are described in the main text (section 5.2.2) and in annex 4 (section 3.21). 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[198]. 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.

12.1 Considerations about migrating and porting

Applications can be broadly qualified in different levels of cloud-readiness:

- *Legacy 'on-premises' applications* that are not candidates for cloudification, for example because they are to be phased out, because their use is too small, or because the technology is too old to migrate them. As an example, an important number of banking applications use still today services written in COBOL, a language popular in the decade of the 60s.

- *Cloud-aware applications*: A cloud aware application is designed or adapted to leverage cloud computing features but nevertheless present challenges that span security, architecture, evolvability, and scalability.

- *Cloud native applications*, specifically designed to benefit from the capabilities of the cloud, such as scalability.

In the public sector, most applications fall within the two first categories: when cloudified/cloudifiable, they are 'aware' but not 'native', which requires important

[198]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.

adaptations (e.g. a re-architecting or a refactoring of the code) when seeking to port them to another cloud service.

There is no one-size-fits-all when migrating (legacy-to-cloud) or porting/switching services (cloud-to-sovereign cloud), as it largely depends on many aspects: the technology used to develop the application, the size, its complexity, or third-party dependencies. This process is not automated and is most often a one-off effort that can hardly be repeated, even if economies of scale can exist. Literature explains the process, both from a technical point of view and a business point of view[199] but there are seldom reports available on the costs associated to migrating or porting/switching, given that this is mostly an ad hoc, one-off activity with many variables interplaying.

At the time of migrating or porting / switching, some key cost elements that should always need to be considered are:

- The size, technology, complexity, and third-party dependencies of the system as-is
- The specificities of the to-be environment.

This will decide how the application will be ported / migrated. In the industry, the 7Rs of migration[200] provide information on what is the most adequate approach for the problem at hand. In legacy-to-cloud and cloud-to-sovereign cloud migration, these are the approaches most commonly followed in the industry:

  - *Rehost or lift-and-shift*, which usually require minimal code changes. This is usually the fastest option to put a service into production, but unless already cloud-native, it incurs into a huge technical debt and post-migration optimization costs. Overall, while the upfront cost of the migration is small, the long-term benefits will be limited, and a large proportion of costs will be spent in optimizing the application to reduce the spendings.
  - *Replatform*, where the application is adapted to managed databases or to other technologies such as containers. This is often the 'by-default' option that offers the stronger Return on Investment (ROI) over time. Also, this is a much more beneficial option in the mid-term than rehosting an application and can lead to significant operational savings.
  - *Refactor*, which requires major or full code rewrites and a new architecture design of the application (e.g. from an n-tier to micro-services or containers), as well as new continuous integration continuous deployment (CI/CD) pipelines, among other considerations. This is a rather costly project and risk-prone, and it is only implemented if the application is expected to deliver large long-term benefits and operational efficiency that outweigh the costs.

[199] Orue-Echevarría Arrieta, L. (2016). From software as a good to software as a service (SAAS): a methodology to define the transformation towards the SAAS business model. Universitat Abat Oliba. https://hdl.handle.net/10803/398024

[200] The 7Rs of migration include the following: *Rehost* (lift-and-shift): Move the application to cloud with minimal changes, *Relocate*: Move VMs without OS or code changes, *Re-platform*: Moderate changes to leverage managed services, *Refactor* (rearchitect): Major or Full rewrite for cloud-native architecture., *Repurchase* (drop-and-shop): Replace with a SaaS equivalent, *Retire*: Decommission application, *Retain* (revisit): Keep on-premises for the time being. Adopted from IBM Strategy

The cost drivers differ depending on whether it is a porting from a cloud service to another (cloud-to-sovereign cloud) or a migration of a legacy application to the cloud. (legacy-to-cloud) The **dominant cost driver of porting an application from one cloud service to another is the labour related to the service re-mapping, re-testing and parallel run in dual infrastructures, and a potential re-adaptation of the application away from proprietary services or older versions of the technologies**. Thanks to the entering into force of the Data Act, egress fees are in the process of disappearing or have already disappeared. Conversely, **when moving a legacy application to the cloud ('cloudification'), the dominant cost is the technical team's labour – architects, software engineers, DevOps - to resolve the technical debt, undocumented dependencies, and architectural incompatibilities with cloud-native patterns, along with the decision to what cloud service to migrate to, both from a technical and a business point of view, and the impact in the organizational processes.** The dual run during the cloudification while critical, does not consume any additional cloud resources, as the legacy application keeps on running on-premises.

Due to the singularity of each migration and porting project and the lack of data from independent resources, the current analysis addresses two distinct migration scenarios in qualitative terms:

> (1) migrating an existing on-premise workload to the cloud (legacy-to-cloud); and
> (2) porting an existing workload from one cloud provider to another (cloud-to-sovereign cloud).

The second scenario is presented in the subsequent sections in quantitative terms. This scope decision reflects a limitation in the available literature: cost data for legacy-to-cloud migrations remains highly variable and context-dependent, making reliable generalisation difficult. Cloud-to-sovereign cloud migrations, by contrast, offer a more stable basis for estimation, as the source environment is often already well documented, the application containerised, and it is operating under known cost parameters, considerations that have been used for the quantitative modelling presented in the next sections.

While both scenarios follow the same broad phases, the effort intensity of the individual activities within each phase of a migration project – that is, how much labour would be dedicated to that specific activity - differs considerably depending on whether the project is a legacy-to-cloud or a cloud-to-sovereign cloud migration. The table below provides a qualitative comparison of the effort intensity per main activity across both scenarios.

Table 65. Comparative table of the intensity effort (qualitative) needed to migrate applications legacy-to-cloud and cloud-to-sovereign cloud (Source: European Commission)

Activity	Legacy-to-cloud effort intensity	Cloud-to-sovereign cloud effort intensity
Architecture design	Medium / High	Low
Refactoring and code migration	High	Medium
Data migration	High	High
Service re-mapping	N/A	High
Testing and validation	High	Medium
Parallel operation (dual run)	Low	Medium
Tooling and licenses	Medium	Low

Activity	Legacy-to-cloud effort intensity	Cloud-to-sovereign cloud effort intensity
Training in new technologies	Medium / High	Low

Some considerations on the above effort intensities:

- **Architecture** is medium / high in legacy-to-cloud: mapping undocumented dependencies of on-premise software is genuinely complex, often requiring reverse engineering techniques. The output is however well defined; it is a target architecture and a wave plan (migration plan). In cloud-to-sovereign cloud the effort intensity in architecture is lower, because usually the application deployment and cloud architecture are already often well documented and reverse engineering techniques, if needed, are much less effort consuming. In this case, the main challenge faced by the architects is to achieve a well and clear structured service-to-service mapping rather than a service discovery and identification from scratch.

- **Refactoring and code migration** is high in legacy-to-cloud. Resolving technical debt, refactoring the code, changing the programming language and technologies, the application of cloud-native or cloud-aware patterns (e.g. load balancers), containerising monoliths or n-tiers, and creating CI/CD pipelines from scratch, represent the hardest engineering work in the entire migration and the one most prone to scope expansion when hidden dependencies surface in the middle of the project. In cloud-to-sovereign cloud this effort is considered to be medium, because the application is already cloud-native or cloud-aware. Here, the work is mainly adaptation, not transformation.

- **Service Re-mapping** is high in cloud-to-sovereign cloud and not yet applicable in legacy-to-cloud. Translating proprietary managed services across platforms demands deep simultaneous knowledge of both providers, and incompatibilities in data models or execution environments could trigger some re-engineering that was invisible at planning time. This is why it is critical to carry out this mapping in earlier phases of the migration.

In any case, the migration or porting should be balanced against the costs of not doing anything:

- **Maintaining legacy applications carries a real and often underestimated cost.** Beyond the direct expense of keeping ageing infrastructure operational, including on-premise data centres that frequently fall short of modern standards, organisations must continuously maintain all dependent software components, manage growing security and vulnerability exposure, and remain with a shrinking pool of engineers who retain the relevant skills as technologies become obsolete. Legacy systems also impose additional overhead cost: the older the application, the more difficult and expensive it becomes to modify, extend, or integrate, progressively limiting an organisation's ability to respond to changing requirements.
- **Remaining with a non-sovereign provider poses a dependency risk not without cost.** Vendor lock-in forecloses the price competition that periodic provider switching would otherwise enable. More significantly, a non-sovereign service

exposes the organisation to geopolitical risk: a provider subject to third-country jurisdiction may face legally compelled data access requests or pressure to degrade service quality, neither of which the customer can effectively resist or even anticipate. These risks carry a cost, whether measured in compliance exposure, quality of service or the political cost of dependency, that cannot be easily quantified.

The final decision follows a total cost of ownership approach and, in addition to the above, would also have to consider aspects such as the acceptance of the technical debt, the level of dependencies from third-party libraries or proprietary source code, the business case, the return of investment or the risk appetite. As explained above, this decision needs to be taken ad-hoc for each application to be ported or migrated. The prioritization of which applications should be ported is a business-driven decision, often based on which application would report a quicker and bigger return on investment (ROI).

12.2 Cost modelling for public administrations to port services (cloud-to-sovereign cloud)

A cost analysis has been carried out to estimate the expenditure involved in porting an application from one cloud service offered by a cloud service provider to another that is functionally equivalent but either provided by another provider or being the same provider, under another type of technical and legal construct.

Published literature on this subject is scarce, largely owing to the highly context-specific nature of cloud migrations: most available sources are online, deal in broad ranges, and provide little explanation of the underlying cost drivers, or the methodology used to derive their estimates the phases considered for the migration, or the type and size of the application ported.

Despite these limitations, and in the absence of more rigorous or detailed benchmarks, these online sources remain the only externally available reference point against which the results of this analysis can be validated. They have therefore been used as cross-validation references, with appropriate caution, alongside resources consulted in confidence from existing projects. Given the inherent uncertainty in this type of estimation, a min-max sensitivity analysis has also been conducted to illustrate the plausible range within which porting costs may fall depending on the application characteristics and migration approach.

The starting point for this assessment is that sovereignty risk assessment will identify public sector IT systems that will need to be ported to sovereign cloud services of at least sovereignty level 2. To follow a conservative approach, it is assumed that derogations will be exceptional. Moreover, it is assumed that the porting will be from one cloud service to one cloud service (1:1 cardinality). Migrating to multiple cloud services at the same time would add an important layer of complexity and risk to the project[201]. Most EU public

[201] Alonso, J., Orue-Echevarria, L., Casola, V. *et al.* Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. *J Cloud Comp* **12**, 6 (2023). https://doi.org/10.1186/s13677-022-00367-6

administrations are still in the process of adopting cloud services[202] under a "cloud first approach"[203], and while deploying workloads following a multi-cloud[204] strategy is a plausible one, this is still a marginal practice.

While it has been reported by Member States in various events (e.g. Member States Cloud Coordination Group (MSCCG) as part of the European Alliance for industrial data, edge and cloud) that the migration from on-premise applications to cloud-aware and cloud-native is growing, there is few available public data that clearly quantifies this growth. France reported in 2025 EUR 84 m of public procurement for cloud - in State administration, healthcare, local administrations, budget operators, public establishments or similar, authority or institution - with an annual growth of 62%. The report stresses that these values stem mostly from small projects and a handful of large ones, positioning France in a cloud adoption trend[205]. Spain and Germany are investing in their own governmental clouds, NubeSara (EUR 84 m[206]) and Deutscheverwaltungslcoud respectively but there is no clearly available disaggregated information on the number of workloads on the cloud. The UK, through its G-Cloud offering reports an expenditure of £400 m in hosting services in fiscal year 2024/2025[207].

[202] See France as an example, in their document Bilan de la doctrine cloud au centre where it is stated: "La dynamique actuelle d'arrivée de nombreux petits projets montre que nous sommes toujours dans une phase d'adoption" (p.6). This can be extended to various MS, which as part of their RRF plans are in the process of migrating their legacy applications to cloud-aware and cloud-native architectures.

[203] See for instance Spain, with its approach "hybrid cloud first" here and here

[204] There are several ways to define multi-cloud. Alonso, Orue-Echevarria et al (2023) concluded in their Systematic Literature Review (SLR) which analysed 88 sources from an initial set of 1 000 papers that multi-cloud applications can be characterized as follows: (a) *Replicated multi-cloud applications* are deployed across multiple clouds sequentially rather than simultaneously. They migrate between providers for economic or operational reasons, such as for cost optimisation, backup needs, emergency failover, or contract expiry. They are purpose-built to run on, and transition between, different cloud environments. The primary concern is seamless switching between providers, making data portability and interoperability central design requirements. (b) *Distributed multi-cloud applications* run subcomponents concurrently across resources from multiple providers, drawing on several independent cloud services in combination. This simultaneous multi-provider model delivers tangible benefits including high availability, fault tolerance, and cost efficiency. It is typically adopted when no single provider offers the full functionality an application requires, allowing organisations to selectively consume the services best suited to their needs within given cost constraints. However, this approach introduces significant complexity: security governance becomes harder to enforce, operational management grows more demanding, and the distributed architecture raises design-phase challenges such as the partitioning of application logic and data across provider boundaries. (c) *Hybrid multi-cloud applications* encompass both of the above patterns: combining the sequential provider usage characteristic of replicated deployments with the concurrent, multi-provider model of distributed architectures, offering the broadest flexibility but also the greatest management overhead.

[205] Bilan de la doctrine cloud au centre

[206] España digital 2026 with a breakdown of the services at Boletín Oficial del Estado, mainly targeting computation power, network and storage.

[207] See G-Cloud tab, select "central government", fiscal year "2025 – 2025"

12.3 Phases of a porting operation

Next, the different phases are described, adapted from the few existing resources in the literature[208] [209] [210] [211] [212].

Phase 1 – Feasibility assessment (one-off adjustment costs): The first step before tackling the porting is to have a clear understanding of the problem that the application is solving, perform a technical feasibility analysis to understand well the complexity, the size, dependencies as well as the technology, architecture, licenses, compliance requirements and quantity of data. In addition, it is important to have a clear understanding of what are the features and technologies accepted by the target service as this will determine the decision on which porting model will be followed.

The following activities have been quantified under this phase taking as input the information provided above and consultation with experts and practical experience in the field:

- Discovery tooling and licensing
- Infrastructure inventory
- Dependency mapping
- Total Cost of Ownership (TCO) analysis

Among the most important challenges to be faced in this step is to underestimate the dependencies across modules (end-to-end calls), the lack of documentation which may result in an incomplete inventory and data classification gaps, underestimating the existence of Personal Identifiable Information (PII) or regulated data in unexpected components requiring at a later stage, for instance a DPIA.

The main outcomes of this phase is a porting inventory, a dependency graph, risk register, and a porting readiness assessment report.

Phase 2 – Strategy and planning (one-off adjustment costs): The second step of the porting is the development of the porting strategy and the planning itself. At this stage, once the characteristics of the application and the target platform are known thanks to the first step, it is a matter of deciding, based on the 7Rs of porting, what is the most adequate approach for the problem at hand: rehost, re-platform or refactor, as the most widely used.

---

[208] Andreas Menychtas, Kleopatra Konstanteli, Juncal Alonso, Leire Orue-Echevarria, Jesus Gorronogoitia, et al.. Software modernization and cloudification using the ARTIST migration methodology and framework. Scalable Computing : Practice and Experience, 2014, 15 (2), pp.131-152. ⟨10.12694/scpe.v15i2.938⟩.
[209] J. Alonso, L. Orue-Echevarria, M. Escalante, J. Gorroñogoitia and D. Presenza, "Cloud modernization assessment framework: Analyzing the impact of a potential migration to Cloud," *2013 IEEE 7th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems*, Eindhoven, Netherlands, 2013, pp. 64-73, doi: 10.1109/MESOCA.2013.6632736.
[210] Orue-Echevarría Arrieta, L. (2016). From software as a good to software as a service (SAAS): a methodology to define the transformation towards the SAAS business model. Universitat Abat Oliba. https://hdl.handle.net/10803/398024
[211] Pahl, C., Xiong, H., Walshe, R. (2013). A Comparison of On-Premise to Cloud Migration Approaches. In: Lau, KK., Lamersdorf, W., Pimentel, E. (eds) Service-Oriented and Cloud Computing. ESOCC 2013. Lecture Notes in Computer Science, vol 8135. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40651-5_18
[212] P. Jamshidi, A. Ahmad and C. Pahl, "Cloud Migration Research: A Systematic Review," in *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 142-157, July-December 2013, doi: 10.1109/TCC.2013.10.

Each option has different consequences in the effort needed to port, the timeline and the risks.

Once one of the above strategies have been decided upon – this can be unique for the complete application or alternatively each part of the application may undergo a different strategy - , the next activities include grouping the workloads into migration waves[213], addressing the identified dependencies, mapping the source services with the target services, re-architecting where needed, define the data porting strategy (e.g. bulk, transfer, incremental, …) as well as setting up the porting programme team. As part of this activity, it is also important to keep a rollback mechanism defined in case the porting does not succeed.

These are the activities evaluated in this phase:

- Cloud architecture design
- Porting plan
- Provider (target platform) feature evaluation and service re-mapping
- Project management setup

The main challenges in this phase stem from the gap in the team skills and the lack of one-to-one match across the functionalities of the various cloud services. That is, while cloud services may theoretically be similar or may have an equivalent functionality, there is not a one – to – one match. This matching must be often manually performed therefore by the team members start carrying out the porting.

The outcomes of this phase are the porting strategy document, the plan, the target architecture design and topology and the RACI[214] matrix.

Phase 3 – Target environment set up (one-off adjustment costs): This step includes the provision and configuration of the infrastructure (e.g. the Virtual Machines), implementing the basic security policy measures (e.g. identity provider), observability environment and logs, the CI/CD pipelines and the Infrastructure-as-Code (IaC) practices on the target environment.

Under this phase, these are the activities considered:

- VM / compute provisioning
- Network configuration (Virtual Private Cloud, DNS, Firewall)
- Storage setup
- Identity and Access Management, access and monitoring setup
- IaC scripting and DevOps pipelines

[213] A migration wave breaks down migration projects into more manageable batches for synchronized and concurrent migration. This is an iterative approach that allows organizations to minimize business disruption and risk, as well as incorporate the lessons learned from the previous wave into the next one.
[214] Responsible, Accountable, Consulted, Informed

The main obstacles in this phase have to do with the potential differences in the Identity and Access Management (IAM) roles and permissions, overlapping IPs, the setup of tools such as security scanning tools or a SIEM (Security Information and Event Management).

The outcomes of this phase are the network topology, the IAM baseline and the DevOps pipeline.

Phase 4 – Porting (one-off adjustment costs): This phase entails the porting of both the business logic of the application as well as the data, while maintaining the integrity, full auditability and minimal downtime of the application. The porting of data may be rather challenging, in terms of duration, strategy, and risks and they require a verification of the integrity of the data at destination (e.g. row counts, checksum, etc) as this is a very error-prone activity. Migrating the business logic may involve refactoring part of the code, re-adapting to new technologies, moving and / or rebuilding the images for the containers, adapting the Kubernetes manifests, redeploying them and reconfiguring certain parts of the application such as the managed services (e.g. load balancers). This step also includes some smoke tests (initial tests) to demonstrate that the application is functional and responsive.

Following, the activities considered:

- Database porting
- VM/server image replication
- Application code adaptation (refactoring) and configuration for porting
- Porting of the tooling licenses
- Parallel infrastructure dual - run

The main problems usually faced during this phase is the data format compatibility, the maintenance of the integrity of the data and the avoidance of data loss during the porting. In terms of application, the integrability and reconfiguration of the different components migrated onto the target platform may hinder the deployment of the application.

The deliverables after this phase is the data and application migrated onto the cloud, and the application deployment view.

Phase 5 – Testing and validation (one-off adjustment costs): This step includes the functional and non-functional testing, including performance, load, stress and resilience testing. Security, vulnerability and penetration testing are also part of this. At this stage, there is a disaster recovery plan in place and clear metrics to ensure business continuity.

These are the activities taken into account under this phase:

- Functional testing
- Performance and load testing
- Integration / API testing
- Security and vulnerability scanning
- Rollback plan validation

The main obstacles in this phase entail usually the test coverage and the responsiveness of the application in extreme conditions. Another key aspect is that the targeted application must mirror in functional terms the migrated one so there has to be a parallel run of both applications for a certain period of time in order to define errors before it goes into production.

The outcome of this phase is the test results from the different tests carried out.

Phase 6 - Cutover and Switching DNS (one-off adjustment costs): This is the most critical phase as it involves the switching from the 'old' environment to the target environment. When going on production, the DNS records are switched, the application health needs to be ensured, and the code is frozen. The definition of a rollback mechanism is also part of this activity.

The tasks included under this phase are:

- DNS / traffic cutover
- Final data synchronization and delta transfer
- Go live
- Downtime window management
- Incident response and hotfixes

The challenges of these activities relate to the DNS switching and how stateful sessions are being handled, that is active user sessions could be lost due to the cutover. The outcome of this phase is the application in production.

Phase 7 – Post – porting (one-off adjustment costs): After a successful cutover, the source environment will still be running but on standby to identify potential performance problems in production. This parallel run is usually for a certain amount of weeks, for example, 2-4 week, even if not the whole time. Moreover, this phase covers the decommissioning of resources, the archiving of the source environment configuration for audit purposes and the update of the architecture documents. Subscriptions or licenses shall also be annulled.

Under this phase the following activities are considered:

- Cost optimization, performance and right-sizing (FinOps)
- Monitoring and alerting setup
- Old infrastructure decommissioning
- Staff training and knowledge transfer

The main challenges include the decommissioning of the source before the rollback window expires risking permanent data loss as well as the engineers who led the porting moving on before the documentation is complete. The outcome of this phase is an application that is operational.

Phase 8 – Operation of the cloud service (recurring adjustment); This phase includes the operation of the service, including observability, performance optimization, FinOps, continuous vulnerability assessment, and maintenance of a functional application (e.g. correction of bugs but also new features being deployed).

12.4 Aspects considered for the analysis of costs

Since not all use cases have the same complexity, for this impact analysis three types of applications are assumed: small, mid-sized, large, as described below. The criterion are industry standard values and were cross referenced with confidential sources:

Table 66. Application taxonomy used for this impact analysis

Criterion	Small application	Mid-size application	Large application
Code base	<10k lines, n-tier (cloud-aware), small number of microservices (cloud-native)	10k – 100k lines, 10 – 20 microservices	>100k lines, > 20 microservices or smaller in number but complex microservices
Data volume	< 100 GB	100 GB – 10 TB	10 TB – PB
Third party dependencies	Few (1-3)	Moderate (5 – 15)	High (>20 or tightly coupled)
Users	< 500 users / < 50 concurrent	500 – 10,000 users / 50 – 500 concurrent	> 10,000 users / > 500 concurrent
Team size	Small	Medium	Large
Typical Estimated Timeline	1 – 3 months	3 - 9 months	> 9 months
Example application	Internal tool / Small application	Departmental	Heavy stakeholder based, such as healthcare applications

As noted above, reliable data on the cost of porting or migrating an application between cloud providers is scarce. This scarcity is structural rather than incidental: each porting project is inherently unique, shaped by how the application was originally architected, the technologies involved, the degree of vendor-specific coupling, and the accumulated technical debt. No two porting project present the same cost profile, which makes meaningful generalisation difficult and explains why the literature has not converged on robust benchmarks. The estimates presented in this section represent a best-effort attempt to triangulate and structurally aggregate the limited sources available reporting costs[215].

[215] Cloud migration cost calculator provides a calculator to calculate where the user can insert the type of migration he is targeting (public to public, public to private and to which of the large three hyperscalers, the criticality of the application, the workload size, the data migration size, the migration strategy – rehost, replatform, refactor and other aspects such as observability, landing zone, security hardening, DevOps pipelines, and team training). Cloud Migration Cost Analysis: Lift-and-Shift vs. Refactoring; Software Modernization Costs provides empirical benchmarks from 200+ real-world cloud-to-cloud migration projects out which 35 have reported cost data. This source reports single-point median figures per strategy at enterprise scale, without any distinction per application size Cloudaware: Cloud Migration

These sources follow different methodologies – application size count mapping, server of VM count mapping, porting strategy per application type and empirical benchmarks from real world cloud-to-sovereign cloud porting projects and show certain bias as they are companies that offer porting services. Under these considerations, the structured aggregated ranges of costs for porting applications, irrespectively of rehosting, re-platforming or refactoring due to the lack of disaggregated data, can be considered as follows:

- Small application: EUR 20 000 – EUR 300 000
- Mid-sized application: EUR 100 000 – EUR 500 000
- Large application: > EUR 500 000

Hence, they should be read as informed approximations rather than precise figures. However, these have been cross-checked with confidential information on past and existing re-platform porting projects in the public sector. The baseline used are as follows: porting a small workload is estimated at a value of EUR 20 000 - 50 000, a mid-size application as of around EUR 200 000 while the porting of large application is estimated to cost around EUR 500 000. In terms of effort, confidential sources report that the porting of a large application has been estimated in 1 000 activity days, which has been taken as benchmark. In this case, this application will not only be moved to another cloud service but will also undergo an adaptation of some of the technologies used such as changing the proprietary web server and data bases for an open source alternative. This is also the plausible scenario selected for the modelling for this impact assessment, given that it is the go-to scenario in the majority of the cases.

There is a rationale behind the distinction of sizes of applications. The cost gap between migrating small and large applications is not only just about volume but largely about dependency and architecture complexity. A factor often underestimated in small applications is the refactoring: the code may be small but poorly documented, with a high technical debt. In mid-sized and large applications, the challenge primarily remains in the integration points (e.g. APIs, databases), which are the main cost drivers and dominate the complexity. Tightly coupled applications, or a bad designed microservices architecture along with a lack of or a bad organizational change management process can outrun the technical costs estimate.

The underlying assumptions for the quantification of the costs are detailed next.

- The modelling accounts for the porting of an application deployed on a VM **(IaaS to IaaS)**, but not from PaaS to PaaS or from SaaS to SaaS. While most of the activities may be similar, less literature resources exist in this regard, rendering the estimations highly complicated and uncertain.

- The modelling measures the **porting costs of moving from a public cloud to a sovereign cloud with sovereignty level 2 – 4.** The baseline used for the public

---

Costs in 2026: Complete Guide to Savings, Benefits & Enterprise Planning uses server or virtual machine count rather than application count as the primary sizing unit, which reflects an infrastructure-first (IaaS) perspective well-suited to compute-migration analysis.; Cloud Migration Cost Analysis: Rehost vs. Refactor provides a representative numerical case drawn from their own company, Opsio, which implements migration projects.

cloud is AWS eu-central (Frankfurt) and used the prices provided by the calculator available online at the provider's site (more details on the instance types selected and their associated costs below), with a **+5% price premium. Sensitivity analysis is +12%, -10%[216].**

- The values for the costs are calculated considering a **manual porting process following the traditional software engineering process**, as, even if limited, there exist some literature sources in this regard. However, part of this porting could be performed using AI automatic code generation, Agentic AI [217] [218] [219] or low-code-no-code platforms[220] that could have an impact on the costs. However, given the novelty of this technique and its incipient use there is, for the time being, scarce literature sources on the costs and on its results in terms of benefits and quality of the source code generated[221].

- The **number of affected public essential entities under NIS2 Annex 1** equals to 6 400. However, not all essential entities make a similar use of cloud services. To respond to this situation, the number of essential public entities has been stratified, as depicted next:

    - **High-intensive users of cloud services:** under this category fall national administrations that make an important use of cloud services either because they have a large proportion of applications on the cloud (both cloud-aware and cloud-native) or the number of services that are deployed on the cloud are low but make a high intense use of cloud services. An example of this could be the national tax services. Based on empirical observations on how the EU public sector is structured, the proportion of this type of users is considered as 20%.

    - **Medium intensive users of cloud services**, which include systems from national ministries that are less intensive in terms of cloud usage and some regional authorities / federal authorities that cover for instance healthcare, or tax services (e.g. Autonomous regions of Spain). Based on empirical

---

[216] This range is explained in section 2.3.4 of the main document.
[217] *Agentic AI* is an autonomous system that leverages from specialized AI agents to analyse, refactor, transform, and validate legacy codebases with minimal human intervention. Traditional code generation tools often only suggested snippets of code or the structure of the application, whereas agentic AI promises to manage independently the entire end-to-end migration process, including the decomposition of a monolithic application to migrating to the new language and platform maintaining the full functionality
[218] See IBM, Reimagining the application migration and modernization value-chain: The agentic way
[219] Bandi, A., Kongari, B., Naguru, R., Pasnoor, S., & Vilipala, S. V. (2025). The Rise of Agentic AI: A Review of Definitions, Frameworks, Architectures, Applications, Evaluation Metrics, and Challenges. *Future Internet*, *17*(9), 404. https://doi.org/10.3390/fi17090404
[220] Low code platforms is a software development environment that allows for the development of applications using visual, drag-and-drop interfaces instead of extensive manual coding, leveraging from model-driven design (MDD) and pre-built components. No code platforms follow the same approach as low code platforms but in this case, there is no need to write any line of code. While often used together, low code allows for the inclusion of custom code, whereas no code is more restrictive and focused on non-technical users. Source: IBM
[221] Wang, H., Gong, J., Zhang, H., Xu, J., & Wang, Z. (2025). Ai agentic programming: A survey of techniques, challenges, and opportunities. *arXiv preprint arXiv:2508.11126*.

observations on how the EU public sector is structured, the proportion of this type of users is considered as 40%.

- **Low-intensive users of cloud services,** upon which national ministries with transactional digital public services are included and regional public administrations. It is to be clarified that while the entities that manage water are considered essential services, they are mostly at municipal level, which help reduce the scope. Based on empirical observations on how the EU public sector is structured, the proportion of this type of users is considered as 40%.

- The usage of cloud services has been stratified as per the values above.

- Based on discussions with three distinct sets of public stakeholders that represent ~200 public authorities, the essential entities are considered to have each 1 200 IT services, where 30% of the services are already cloudified and would be effect of a cloud-to-cloud porting, 30% are on-premises and will be cloudified, and 40% should remain on premise (e.g. legacy systems that are being phased out, very small IT services).

- Based on the discussions mentioned above, the distribution of sovereignty needs resulting from the risk assessment across the public sector are Level 1: 70%, Level 2: 20%, Level 3: 9%, Level 4: 1%.

- The effort to migrate a legacy-to-cloud application is estimated to be 1.5x the effort estimated to port a service from cloud-to-cloud, taking as baseline the comparison shown in previous sections.

- The ratio of applications in terms of size and types of cloud intensity users is stratified as shown next. The proportion of small, mid-size and large applications in the case of high-intensive users of cloud services has been obtained from the experience of confidential sources. For medium and low intensive users of cloud services, the values are estimated, taking as anchor value the potential proportion of large applications that there could be in each type of entity.

Table 67. Distribution of types of users of cloud services in public essential entities operating under NIS2 Annex I (Source: European Commission)

	Small App.	Mid-size App.	Large App.	Total
High intensive users of cloud services	50%	45%	5%	100%
Medium intensive users of cloud services	60%	37%	3%	100%
Low intensive users of cloud services	70%	29%	1%	100%

- **Labour costs** are considered as average costs of EUR 75 / h, irrespective of their profile (cloud architect, developer, DevOps engineer, project manager or external consultant). These costs are higher than the ones considered in the rest of the impact assessment, given the large number of profiles participating in a porting of an application.

- Out of the three approaches presented beforehand, the '**re-platform'** option has been selected, as being the most plausible one, since it combines porting the application as-is, creating cloud-agnostic components that can facilitate a future porting to another service provider and other common activities such as some adaptations some of the used technologies or a small refactoring of the code.

- For the calculations on the **pricing of VMs and storage**, comparing sovereign solutions level 2 and sovereign solutions level 3 / 4, internal knowledge has been considered, complemented with desk research data that report, through use cases and empirical analysis, similar prices for computation resources (VM, storage, network)[222] [223].

- Switching charges are considered to be null, as an effect of the Data Act.

- For each of the application sizes, the following number of VMs and sizes are considered. Pricing is based on AWS EC2 on-demand rates in eu-central (Frankfurt) in USD (1 USD rounded to 0.9 for EUR for the conversion), and dedicated instances (Prices of March 2026). The rationale for the decision of the instance types is provided next.

    - T-series such as t3 are burstable instances, which provide a baseline level of CPU and can burst above when needed. They are recommended for workloads with variable CPU usage such as small web servers or microservices that mostly idle but have occasional spikes.

    - M5-series are often used as the *default* instance type for applications that need consistent CPU performance and that do not fit into compute or memory-optimized type of applications. M5 instances are balanced CPU and memory instances, designed for midsize databases and back-end applications. M-instance types are at the crossroads of T (general purpose), C (compute-optimized) and R (memory-optimized) instance types in terms of compute and memory allocation.

    Both T and M instance types are considered General Compute.

Table 68. Types of VMs considered for the cost estimations for small, mid-size and large applications (Source: European Commission based on AWS Calculator, March 2026)

[222] See for example this reported experiences https://european.cloud/2025/06/a-basic-look-at-pricing-of-european-cloud-vendors/ , https://www.dataminded.com/resources/cloud-independence-testing-a-european-cloud-provider-against-the-giants, https://www.fromeuropewithlove.eu/en/blog/european-cloud-providers-vs-aws-comparison-2026
[223] BCG

Parameter	Small	Mid-Size	Large	Baseline metric
Instance Type	t3.large	m5.xlarge	m5.8xlarge	AWS EC2, Dedicated instance, EBS gp3, eu-central (Frankfurt)
VM Count	1–3	3–5	5-10	VMs per app
vCPU	2	4	32	cores
RAM	4	16	64	GB
Network bandwidth	Up to 5	Up to 5	Up to 25	Gbps
Price	0.12	0.39	3.09	EUR/h

As anticipated above, across all, labour costs represent the largest component irrespective of it being legacy-to-cloud or cloud-to-sovereign cloud, and in all phases. The calculation of the labour effort stem from the few available sources and estimations provided in confidence by experienced personnel of the public sector who have tackled complex porting projects.

Table 69. Estimation of effort incurred in a porting, cloud-to-sovereign cloud, broken down in phases (central values)

Porting phases Sovereign Cloud	Small application (hours)	Mid-size application (hours)	Large application (hours)
Phase 1 – Feasibility assessment	40	290	470
Phase 2 – Strategy and planning	75	470	1,060
Phase 3 – Target environment set up	28	205	540
Phase 4 – Porting	173	1,496	3,860
Phase 5 – Testing and validation	64	640	1,200
Phase 6 - Cutover and Switching	16	128	410
Phase 7 – Post – porting and decommission	12	108	460
Total one-off effort (hours)	**408**	**3,337**	**8,000**

As mentioned above, the effort for legacy-to-cloud migration is 1.5x the effort shown above.

The min-max values considered, and their explanation are as follows:

Table 70. Estimation of effort incurred in a migration, min-max values

Migration phases Sovereign Cloud	Small application (hours) [min value, max value]	Mid-size application (hours) [min value, max value]	Large application (hours) [min value, max value]	Rationale
Phase 1 – Feasibility assessment	[26, 54]	[180, 400]	[300, 640]	Given the importance of all the activities under this

Migration phases Sovereign Cloud	Small application (hours) [min value, max value]	Mid-size application (hours) [min value, max value]	Large application (hours) [min value, max value]	Rationale
				phase, experience demonstrates that a good understanding of the application (assets, dependencies, licenses) are equal and their effort varied.
Phase 2 – Strategy and planning	[50, 100]	[332, 608]	[760, 1360]	While all values are increased, the main driver for this change is the cloud architecture design. This is a critical activity that, if not performed properly, can result in over-costs in the migration and operation phase, as it can cause over costs.
Phase 3 – Target environment set up	[18, 38]	[138, 272]	[380, 700]	VM provisioning and configuration is the main effort intense activity in this phase. Configuring the security policies or the computation resources in an incorrect way can result in cost inefficiencies. A common error in this phase is to over-provision capacity to be able to respond to potential load spikes.
Phase 4 – Migration	[110, 236]	[860, 2 132]	[2 200, 5 520]	The main drivers in this phase are the migration of the data and the adaptation of the application. The success of these activities largely depends on the previous activities

Migration phases Sovereign Cloud	Small application (hours) [min value, max value]	Mid-size application (hours) [min value, max value]	Large application (hours) [min value, max value]	Rationale
				such as the dependency assessment or the cloud architecture design and service mapping. Moreover, the skills of the team and the wave plan have also a large effect in the effort needed for the migration of the code.
Phase 5 – Testing and validation	[42,87]	[440, 840]	[700, 1 700]	All testing activities considered (functional, integration and performance) are driving the min – max values in this phase. The decision of the coverage of the tests plays an important role. A low coverage testing will result in more bugs during production. Correcting errors during production are much more costly and can have further implications if an efficient CI/CD pipeline has not been well implemented.
Phase 6 - Cutover and Switching	[10, 22]	[90, 166]	[280, 540]	The variation mainly stems from the final data migration and the process of going into production.
Phase 7 – Post – migration and decommission	[8, 16]	[68, 148]	[280, 640]	Under this phase, the most important activities that drive the increment are setting up the observability mechanisms, the

Migration phases Sovereign Cloud	Small application (hours) [min value, max value]	Mid-size application (hours) [min value, max value]	Large application (hours) [min value, max value]	Rationale
				decommissioning of the infrastructure and verifying that everything was correct, and the training of the staff that will be operating the application.
Total one-off effort (hours)	**[264 - 553]**	**[2 108 – 4 566]**	**[4 900– 11 100]**	

The remaining costs of a migration / porting span infrastructure (VM), tooling licenses, and the cost of parallel running both environments during transition. The table below shows the values considered for the min-max approach.

Table 71. Estimation of VMs in the different migration phases (min, max, central values)

Phase	Small	Mid-sized	Large
P3 - Target Environment Setup	**VM provisioning:** ranges between 3 and 6 days [only working hours in 3 weeks]	**VM provisioning:** ranges between 6 and 9 days [only working hours in 3 weeks]	**VM provisioning:** ranges between ranges between 9 and 12 days [only working hours in 3 weeks]
P4 - Migration	**VM / server image replication**: ranges between 3 and 6 days [only working hours in 3 weeks] **Parallel infrastructure (dual-run):** ranges between 8 and 16 days [only working hours in 8 weeks]	**VM / server image replication:** ranges between 6 and 9 days [only working hours in 3 weeks] **Parallel infrastructure (dual-run):** ranges between 16 and 24 days [only working hours in 8 weeks]	**VM / server image replication:** ranges between 9 and 12 days [only working hours in 3 weeks] **Parallel infrastructure (dual-run):** ranges between 16 and 24 days [only working hours in 8 weeks]

Phase	Small	Mid-sized	Large
P6 - Cutover and Switching	**Go live activity:** given the criticality of this activity, no ranges are considered. Duration 2 weeks, 24/7	**Go live activity:** given the criticality of this activity, no ranges are considered. Duration 2 weeks, 24/7	**Go live activity:** given the criticality of this activity, no ranges are considered. Duration 2 weeks, 24/7
P7 - Post-Migration	**Optimization:** given the criticality of this activity, no ranges are considered. Duration 2 weeks, 24/7	**Optimization**: given the criticality of this activity, no ranges are considered. Duration 4 weeks, 24/7	**Optimization:** given the criticality of this activity, no ranges are considered. Duration 4 weeks, 24/7

One-off adjustment costs for the porting and migration of cloud services (legacy-to-cloud, cloud-to-cloud) incurred by public essential entities listed under NIS2 Annex I

Based on the consideration above, namely:

- 6 400 entities, classified in high-intensive users, medium intensive users, and low intensive users of cloud services, distributed as explain above.
- 1 200 IT services are considered, where 30% of the services are already cloudified and would be subject to a cloud-to-cloud migration, 30% are on-premises and will be cloudified, and 40% should remain on premise (e.g. legacy systems that are being phased out, very small IT services).
- Three types of IT services depending on the size and complexity, small, mid-sized and large, distributed as explained previously.
- Based on the discussions mentioned above, the distribution of sovereignty needs resulting from the risk assessment across the public sector are Level 1: 70%, Level 2: 20%, Level 3: 9%, Level 4: 1%.
- The effort to migrate legacy-to-cloud is 1.5x bigger than porting cloud-to-cloud.

The total estimated costs of porting cloud – to – cloud for different sovereignty levels (1-4, 2-4) is shown in the table below. For sensitivity purposes, a baseline for the price markup of sovereign services over current cloud offerings has been set in +5% and a range from + 12% to -10% is considered[224].

[224] Rationale for the range is described in section 2.3.4. of the main document.

Table . Cloud-to-sovereign cloud porting costs (m EUR) of the IT systems of NIS 2 public essential entities for different price markups and sovereign assurance levels (Sovereignty Assurance Level (SAL) 1-4, SAL 2-4)

IT system SAL	Max (+12%)	Base (+5%)	Min (-10%)
SAL 1-4	288,423	287,629	285,158
SAL 2-4	86,527	86,289	85,547

As shown in the tables above, the price markup of sovereign solutions does not influence significantly the cost of porting or migration as most of this cost comes from the human effort to run that activity.The central EUR 86.3 bn figures should be regarded as a maximalist estimate of the potential cost of porting applications to sovereign cloud services on levels 2-4 across around 6 400 public entities. This estimate assumes that 30% of the cloudified solutions of these entities, all those requiring sovereignty assurance levels 2 to 4, would be subject to porting because of the intervention. Moreover, this estimate corresponds to a "big bang" implementation scenario, whereby all 6 400 entities would undertake the porting activities in the first year. In practice, this scenario is unlikely to reflect the actual phases of implementation, as the porting process would typically be expected to occur progressively over a longer period, possibly extending up to five years. Finally, this cost estimate cannot be fully attributed to the policy intervention itself. A significant share of this porting would likely arise anyway as a result of natural procurement decisions taken by public authorities over time, including routine renewal, replacement or migration of cloud services. Treating this full amount as an incremental cost of the intervention therefore overstates its direct impact.

Accordingly, under PO2-C, a more proportionate estimate has been considered. While remaining conservative, as it continues to include 6 400 entities for potential porting costs, it considers only a subset of critical applications for which porting to cloud services with sovereign levels 3-4 could be directly accelerated by the policy intervention. This would correspond to an anticipated range of 1% of applications in the minimum scenario (that considers porting of all SAL4-demanding applications) up to 6% in the maximum scenario (including also the porting of a good part of SAL3-demanding services), ported over 3 years. On this basis, the estimated cost under this option would amount to approximately EUR 2.5bn in the minimum scenario and EUR 14.8 bn in the maximum scenario. These figures are calculated as the sum of discounted values over a three-year period, following a natural progressive migration approach, starting in 2030 and using 2025 as the baseline year.

Under PO2-B, the measures are not mandatory and would thus be expected to apply to a smaller number of public authorities. For this option, the relevant number of entities is assumed to be around 1 600 public authorities, i.e. 25% of the ones considered under PO2-C. As a result, the associated porting costs are assumed to decrease proportionally to 25% of the PO2-C estimates, amounting to around EUR 620 m in the minimum scenario and EUR 3.7 bn in the maximum scenario.

Recurring operating costs

Operating a cloud service requires a continuous monitoring and optimization. Under this impact assessment and in line with industrial practices, operating an IT system on the cloud involves also the release of new features.

Some of the main activities under the operation phase include release engineering, infrastructure provisioning, and observability, with each one generating their own expenses, even if they all are highly interdependent.

Release pipelines offer the earliest opportunity for cost control. Every execution consumes ephemeral compute and produces artifact storage, which means that improvements to build reliability and release validation compound in quick manner. Organizations that invest in release discipline by reducing failure rates, tightening validation gates, and minimizing rollbacks, consistently achieve lower pipeline costs than those running at higher deployment velocity without equivalent quality controls. The returns are direct and measurable.

Infrastructure provisioning, typically the largest cost category, responds well to deliberate management. Virtual machines can be right sized to match actual utilization patterns, eliminating the idle compute overhead that accumulates when capacity is provisioned conservatively. Monitoring agents while often overlooked, are similarly important to rationalization. They allow to reduce the overhead per-host that otherwise would scale independently of the application workload. regardless of application load. Organizations that treat infrastructure sizing as an ongoing practice rather than a one time decision tend to maintain materially lower baseline costs.

The estimated effort in hours for operating a cloud service, considering also the addition of new features and continuous optimization, per type of application is shown in the next table. This estimation is based on experiences from industry experts.

Table . Estimated effort to operate and maintain a cloud service (hours)

Migration phases Sovereign Cloud	Small app	Mid-size app	Large app
Phase 8 - Operation	968	4.840	6.600

12.5 Limitations of the analysis

The cost model presented in this analysis carries several important limitations that must be acknowledged when interpreting its outputs. First, labour rates are modelled as a static band (EUR 75/hr) that does not account for overtime, or additional consultant charges. Second, VM configurations are drawn from tier averages rather than empirically measured utilization profiles, which is the proper way of estimating the sizes, introducing upward bias notably in the infrastructure costs assumed for Phase 3 and Phase 4 through implicit over-provisioning, reflected in the VMs chosen. Third, all infrastructure pricing uses AWS public cloud on-demand rates as a baseline. On-demand instances are on the costly end. Fourth, the two-month parallel infrastructure (dual-run) window in Phase 4 is fixed to several days a week for a longer period of time. This is however one of the riskiest phases that would need to be estimated proportionately and accurately on a case-by-case basis. However, while fixed to several days, these have been estimated considering industry's best practices. Finally, the cost ranges are based on benchmarks that present total costs of migration, aggregating labour, infrastructure, training, and tooling licensing. Again, this is largely dependent on the as-is situation and the to-be situation.

ANNEX 13. COMPARATIVE ANALYSIS OF SELECTED CLOUD SERVICES

European cloud providers offer far narrower service catalogues than US hyperscalers: AWS alone spans over 200 distinct services. Yet this gap is less consequential than it appears. The latest Eurostat data for 2025 shows that the services EU enterprises actually rely on most are email, office software, file storage, database hosting, and compute power[225], which are primarily IaaS and SaaS. Compute power, hosting, file storage and database are the basis for core IaaS workloads: virtual machines, managed databases, storage, and nowadays also PaaS, where managed Kubernetes (orchestration) are robustly available across European providers. Email and Office software are SaaS. Given the heterogeneity of SaaS, which is much larger than in IaaS and PaaS, and where each application on the web could be called, even if in simplistic terms, software as a service, renders the comparison between US and EU providers, albeit a few exceptions, much more difficult.

However, the **real gaps are narrower and more specific** that it can be initially thought. These include mainly **native AI/ML platforms, serverless, and integrated analytics pipelines** as they remain areas where European providers have not yet reached hyperscaler maturity but are working towards it. For the **standard private and public sector workloads constituting nowadays the majority of cloud adoption needs, the European providers represent already a fully viable, equivalent in performance, functionalities and quality**.

The tables below show that major European cloud providers, for the purpose of this analysis, IONOS, OVHcloud, and STACKIT, already offer services broadly equivalent to those of AWS, Microsoft Azure, and Google Cloud Platform across the core infrastructure categories that are most widely used: compute, storage, network, and managed container orchestration. The comparison has been extended to office automation suites, one of the most widely adopted SaaS categories in the public sector, where credible European and open-source alternatives are also available.

OVHcloud's[226] portfolio spans across compute, storage, networking, container orchestration, databases, analytics, and AI/ML services. IONOS[227] mainly covers storage, compute, managed container orchestration, databases, and observability. STACKIT's[228] catalogue includes compute, databases, observability and logging, and security services. Taken together, these providers cover the functional surface that the majority of the private and public sector workloads actually require.

The comparisons shown below demonstrate that EU providers already offer the most used services and with a similar level of functionality. The first table aims to provide a high-level overview of the main cloud services used in the Union and their coverage by EU providers compared to non-EU incumbents. In the public sector, interviews have shown

---

[225] See Eurostat
[226] OVH
[227] Ionos
[228] Stackit

that most public administrations use an average of twenty services, instead of the whole range offered by hyperscalers.

Table 74. High level overview of cloud services and their coverage by EU providers

Service Type	Layer	Coverage by EU providers
Virtual Machines / Compute	IaaS	Full
Object Storage (S3 compatibility)	IaaS	Full
Block Storage	IaaS	Full
Managed Load Balancer	IaaS/Network	Full
VPC / Private Networking	IaaS/Network	Full
CDN	IaaS/Network	Partial
Managed containers / containers (Container as a Service - CaaS)	PaaS	Full
Managed PostgreSQL/MySQL	PaaS	Full
Managed NoSQL / MongoDB	PaaS	Full
Managed Kafka / Streaming	PaaS	Full
Serverless Functions (FaaS)	PaaS	Partial
Serverless Containers	PaaS	Partial
AI/ML Training Platforms	PaaS	Partial
Managed AI Inference	PaaS	Partial
ERP	SaaS	Full
Office automation / Collaboration / Messaging	SaaS	Full

The second set of tables provide a much more granular analysis comparing per feature five of the widest adopted services: compute, storage, network, managed containers and office automation tools.

A sample of EU providers have been selected to demonstrate that, also when analysing per functionality, European providers' offerings are equivalent to those provided by non-EU incumbents.

This analysis is based on desktop research, more specifically, through a manual review of each provider's official user guides, technical documentation, and online manuals. Where a service appeared to fulfil the same functionality as its counterpart, but the documentation did not allow for an unambiguous confirmation, the mapping has been marked as partial rather than full. This conservative approach reflects an inherent limitation of the methodology: the analysis is theoretical in nature, derived from published specifications rather than from hands-on testing or validated benchmarking.

Table 75. Comparative table compute (selected sample of providers)

Functionality	AWS EC2	Google Compute	Azure Compute	OVH Compute	IONOS Compute	StackIt Compute
General purpose VMs	✓	✓	✓	✓	✓	✓

Functionality	AWS EC2	Google Compute	Azure Compute	OVH Compute	IONOS Compute	StackIt Compute
Compute-optimized	✓	✓	✓	✓	✓	~
Memory-optimized	✓	✓	✓	✓	✓	~
Bare metal instances	✓	✓	✓	✓	✓ (Dedicated servers)	✕
Custom vCPU / RAM ratio	~	✓	~	~	~ (flexible within tiers)	~ (fixed ratios)
Reserved instances	✓	✓	✓	✓	✓	✕
Confidential compute	✓	✓	✓	~	✕	✓

Legend: ✓ Supported ~ Partial / limited ✕ Not available

Table 76. Comparative table Storage (selected sample of providers)

Functionality	AWS	Google	Azure	OVH	IONOS	StackIt
Block storage (persistent disks)	✓	✓	✓	✓	✓	✓
Object storage integration	✓	✓	✓	✓	✓	✓
Shared / NFS file storage	✓	✓	✓	~	~	~
Snapshot & image management	✓	✓	✓	✓	✓	✓
Multi-zone disk replication	✓	✓	✓	~	~	~
Encrypted storage at rest	✓	✓	✓	✓	✓	✓

Legend: ✓ Supported ~ Partial / limited ✕ Not available

Table 77. Comparative table Network (selected sample of providers)

Functionality	AWS	Google	Azure	OVH	IONOS	StackIt
Virtual private network (VPC)	✓	✓	✓	✓	✓	✓
IPv6 support	✓	✓	✓	✓	✓	✓
Load balancer (managed)	✓	✓	✓	✓	✓	✓
CDN	✓	✓	~	✓	✓	✓
Private interconnect / VPN	✓	✓	✓	✓	✓	~

Functionality	AWS	Google	Azure	OVH	IONOS	StackIt
DNS service (managed)	✓	✓	✓	✓	✓	✓
DDoS protection (built-in)	✓	✓	✓	✓	✓	✓
Floating / elastic IPs	✓	✓	✓	✓	✓	✓

Legend: ✓ Supported ~ Partial / limited ✕ Not available

Table 78. Comparative table Containers (selected sample of providers)

Functionality	AWS (ECS/EKS/Fargate)	Google (GKE/Cloud Run)	Azure (AKS / ACI)	OVH (MKS)	IONOS (Managed Kubernetes)	StackIt (SKE)
Managed Kubernetes service	✓	✓	✓	✓	✓	✓
Serverless / managed container service (non-K8s)	✓	✓	✓	✕	✕	✕
CNCF certified Kubernetes	✓	✓	✓	✓	✓	✓
Vanilla / upstream Kubernetes	~	✓	~	✓	✓	✓
Latest K8s version availability speed	~	✓	~	✓	~	~
Extended version support (LTS)	✓	✓	✓	~	✕	✕
Managed / free control plane	~	✓	✓	✓	✓	✓
High-availability control plane	✓	✓	✓	✓	✓	✓
Multi-AZ control plane	✓	✓	✓	✓	~	~
Dedicated control plane (isolated)	✓	✓	✓	✓	~	~
Automatic control plane upgrades	✓	✓	✓	✓	✓	✓
Private (API server not public)	✓	✓	✓	✓	✓	✓
Cluster self-repair / auto-healing	✓	✓	✓	✓	✓	✓
Multiple clusters per project	✓	✓	✓	✓	✓	✓

Functionality	AWS (ECS/EKS/Fargate)	Google (GKE/Cloud Run)	Azure (AKS / ACI)	OVH (MKS)	IONOS (Managed Kubernetes)	StackIt (SKE)
Multiple node pools per cluster	✓	✓	✓	✓	✓	✓
Custom node pool sizing (CPU/RAM)	✓	✓	✓	✓	✓	✓
GPU node pools	✓	✓	✓	✓	✓	✕
Spot / preemptible node pools	✓	✓	✓	✓	~	✕
Node auto-repair	✓	✓	✓	✓	✓	✓
Automatic node OS upgrades	✓	✓	✓	✓	✓	✓
Bare metal worker nodes	✓	✓	✓	✓	✕	✕
Cluster / node autoscaler	✓	✓	✓	✓	✓	✓
Horizontal Pod Autoscaler (HPA)	✓	✓	✓	✓	✓	✓
Vertical Pod Autoscaler (VPA)	✓	✓	✓	~	~	~
Event-driven autoscaling (KEDA)	✓	✓	✓	~	~	~
Autopilot / serverless node provisioning	~	✓	~	✕	✕	✕
Scale-to-zero / scheduled shutdown	✓	✓	✓	~	~	✓
VPC / private network integration	✓	✓	✓	✓	✓	✓
Managed load balancer (ingress)	✓	✓	✓	✓	✓	✓
Network policies (CNI)	✓	✓	✓	✓	✓	✓
Cilium CNI support	✓	✓	✓	✓	✕	✕
Service mesh integration (Istio/Linkerd)	✓	✓	✓	~	~	~
IPv6 cluster support	✓	✓	✓	✓	~	~

Functionality	AWS (ECS/EKS/Fargate)	Google (GKE/Cloud Run)	Azure (AKS / ACI)	OVH (MKS)	IONOS (Managed Kubernetes)	StackIt (SKE)
Ingress / Gateway API support	✓	✓	✓	✓	~	~
Private nodes (no public IPs)	✓	✓	✓	✓	✓	✓
Persistent volumes (block storage)	✓	✓	✓	✓	✓	✓
ReadWriteMany (RWX) volumes	✓	✓	✓	~	~	~
Managed NFS / file storage	✓	✓	✓	✓	~	~
Dynamic volume provisioning	✓	✓	✓	✓	✓	✓
Encrypted storage at rest	✓	✓	✓	✓	✓	✓
Volume snapshots	✓	✓	✓	~	~	~
Managed private container registry	✓	✓	✓	✓	✓	✓
OCI & Helm artifact support	✓	✓	✓	✓	✓	✓
Image vulnerability scanning	✓	✓	✓	✓	~	~
Geo-replication of registry	✓	✓	✓	~	×	×
Registry integrated with K8s cluster	✓	✓	✓	✓	✓	✓
RBAC (role-based access control)	✓	✓	✓	✓	✓	✓
OIDC / SSO authentication	✓	✓	✓	✓	~	~
Pod Security Standards (PSS)	✓	✓	✓	✓	✓	✓
Secrets management (KMS integrated)	✓	✓	✓	~	~	~
Network policy enforcement	✓	✓	✓	✓	✓	✓
Image signing / admission control	✓	✓	✓	~	~	~

Functionality	AWS (ECS/EKS/Fargate)	Google (GKE/Cloud Run)	Azure (AKS / ACI)	OVH (MKS)	IONOS (Managed Kubernetes)	StackIt (SKE)
Confidential Kubernetes / TEE nodes	✓	✓	✓	~	✕	✓
Audit logging	✓	✓	✓	✓	~	~
Built-in monitoring (metrics)	✓	✓	✓	~	~	~
Built-in logging	✓	✓	✓	~	~	~
Prometheus / Grafana integration	✓	✓	✓	✓	✓	✓
Alerting & dashboards	✓	✓	✓	~	~	~
kubectl / API access	✓	✓	✓	✓	✓	✓
Terraform / IaC support	✓	✓	✓	✓	✓	✓
GitOps / ArgoCD support	✓	✓	✓	✓	~	~
CLI tooling	✓	✓	✓	✓	✓	✓
Native CI/CD pipeline integration	✓	✓	✓	~	~	~
PaaS / Cloud Foundry layer	✕	✕	✕	✕	✕	✓
Multi-cluster management console	✓	✓	✓	✓	✓	✓

Legend: ✓ Supported ~ Partial / limited ✕ Not available

Table 79. Comparative table Office automation tools (selected marek of providers)

Functionality	Microsoft 365	Google Workspace	Nextcloud + Collabora	OnlyOffice	CryptPad	Infomaniak kSuite	LibreOffice	Open-Xchange
	US Proprietary	*US Proprietary*	*EU Open Source*	*EU Open Source*	*EU Open Source*	*EU Proprietary*	*EU Open Source*	*EU Open Source*
DOCUMENT CREATION & WORD PROCESSING								
Word processor	✓	✓	✓	✓	✓	✓	✓	✓

Functionality	Microsoft 365	Google Workspace	Nextcloud + Collabora	OnlyOffice	CryptPad	Infomaniak kSuite	LibreOffice	Open-Xchange
	US Proprietary	*US Proprietary*	*EU Open Source*	*EU Open Source*	*EU Open Source*	*EU Proprietary*	*EU Open Source*	*EU Open Source*
Advanced text formatting	✓	~	~	~	~	~	✓	~
Desktop application (offline)	✓	✗	✗	✓	✗	✗	✓	✗
Browser-based editing	✓	✓	✓	✓	✓	✓	✗	✓
Mobile editing (iOS / Android)	✓	✓	✓	~	~	✓	✗	~
Track changes / review mode	✓	✓	✓	✓	✗	✓	✓	~
Templates library	✓	✓	~	✓	~	~	✓	~
Mail merge	✓	~	~	✓	✗	✗	✓	✗
Macro support (scripting)	✓	~	✗	~	✗	✗	✓	✗
Digital signatures / e-signing	✓	✓	~	~	✗	~	✗	~
SPREADSHEETS								
Spreadsheet editor	✓	✓	✓	✓	✓	✓	✓	✓
Advanced formulas & functions	✓	~	~	~	~	~	✓	~
Pivot tables	✓	✓	~	✓	✗	~	✓	✗
Macros / VBA support	✓	✗	✗	~	✗	✗	✓	✗
Charts & data visualization	✓	✓	✓	✓	~	~	✓	~

Functionality	Microsoft 365	Google Workspace	Nextcloud + Collabora	OnlyOffice	CryptPad	Infomaniak kSuite	LibreOffice	Open-Xchange
	US Proprietary	*US Proprietary*	*EU Open Source*	*EU Open Source*	*EU Open Source*	*EU Proprietary*	*EU Open Source*	*EU Open Source*
Data validation rules	✓	✓	~	✓	~	~	✓	~
Conditional formatting	✓	✓	✓	✓	~	~	✓	~
Large dataset performance	✓	~	~	~	✗	~	✓	✗
Import/export Excel (.xlsx)	✓	✓	✓	✓	~	✓	✓	~
PRESENTATIONS								
Presentation editor	✓	✓	✓	✓	✓	✓	✓	~
Slide templates & themes	✓	✓	~	✓	~	~	✓	✗
Animations & transitions	✓	~	~	✓	~	~	✓	✗
Presenter view	✓	✓	✓	✓	✗	~	✓	✗
Live audience interaction	✓	~	✗	✗	✗	✗	✗	✗
Export to PDF / video	✓	✓	✓	✓	~	✓	✓	~
Embed media (audio/video)	✓	~	~	✓	✗	~	✓	✗
PPTX import/export fidelity	✓	~	~	✓	~	✓	~	✗
REAL-TIME COLLABORATION								
Simultaneous co-editing	✓	✓	✓	✓	✓	✓	✗	✓

Functionality	Microsoft 365	Google Workspace	Nextcloud + Collabora	OnlyOffice	CryptPad	Infomaniak kSuite	LibreOffice	Open-Xchange
	US Proprietary	*US Proprietary*	*EU Open Source*	*EU Open Source*	*EU Open Source*	*EU Proprietary*	*EU Open Source*	*EU Open Source*
Live cursor / presence display	✓	✓	✓	✓	✓	✓	✕	~
In-document comments & threads	✓	✓	✓	✓	✓	✓	✕	~
Document version history	✓	✓	✓	✓	✓	✓	✕	~
Suggesting / review mode	✓	✓	✓	✓	~	✓	✓	~
Paragraph-locking (conflict free)	~	✕	✕	✓	✓	✕	✕	✕
Link sharing (no-login editing)	✓	✓	~	✓	✓	✓	✕	~
Guest / external collaborators	✓	✓	✓	✓	✓	✓	✕	✓
EMAIL & COMMUNICATION								
Email client / webmail	✓	✓	✕	~	✕	✓	✕	✓
Calendar	✓	✓	✓	~	✕	✓	✕	✓
Contacts / address book	✓	✓	✓	~	✕	✓	✕	✓
Tasks / to-do management	✓	✓	✓	~	✕	✓	✕	✓
Team chat / messaging	✓	✓	✓	~	✓	~	✕	~
Video conferencing	✓	✓	✓	✕	✓	✓	✕	~

Functionality	Microsoft 365	Google Workspace	Nextcloud + Collabora	OnlyOffice	CryptPad	Infomaniak kSuite	LibreOffice	Open-Xchange
	US Proprietary	*US Proprietary*	*EU Open Source*	*EU Open Source*	*EU Open Source*	*EU Proprietary*	*EU Open Source*	*EU Open Source*
Webinar / large meeting hosting	✓	✓	~	✕	✕	~	✕	✕
Screen sharing	✓	✓	✓	✕	✓	✓	✕	~
FILE STORAGE & MANAGEMENT								
Cloud file storage	✓	✓	✓	✓	✓	✓	✕	✓
Desktop sync client	✓	✓	✓	✓	✕	✓	✕	~
Offline file access	✓	~	✓	✓	✕	~	✓	~
External file sharing links	✓	✓	✓	✓	✓	✓	✕	✓
File versioning & restore	✓	✓	✓	✓	✓	✓	✕	✓
Folder-level permissions	✓	✓	✓	✓	✓	✓	✕	✓
Self-hosted / on-premise	✕	✕	✓	✓	✓	✕	✓	✓
Included cloud storage (entry plan)	1TB	15GB	Self-hosted	5GB	1GB	15GB	Local	Self-hosted
AI & PRODUCTIVITY TOOLS								
Integrated AI writing assistant	✓	✓	~	✓	✕	✕	✕	✕
AI email drafting / summarization	✓	✓	✕	✕	✕	✕	✕	✕
AI meeting notes / transcription	✓	✓	✕	✕	✕	✕	✕	✕

Functionality	Microsoft 365	Google Workspace	Nextcloud + Collabora	OnlyOffice	CryptPad	Infomaniak kSuite	LibreOffice	Open-Xchange
	US Proprietary	*US Proprietary*	*EU Open Source*	*EU Open Source*	*EU Open Source*	*EU Proprietary*	*EU Open Source*	*EU Open Source*
AI spreadsheet / formula help	✓	✓	✕	~	✕	✕	✕	✕
No-code app builder	~	✓	✕	✕	✕	✕	✕	✕
Workflow automation	✓	✓	~	~	✕	~	✕	~
Forms / survey tool	✓	✓	✓	✓	✓	~	✕	~
Whiteboard / drawing tool	✓	✓	✓	✓	✓	~	✕	~
Notes / wiki tool	✓	✓	✓	~	~	~	✕	~

Legend: ✓ Supported ~ Partial / limited ✕ Not available