ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

OCCASIONAL PAPER – No. 07/2025

Breaking Barriers to Cloud Customer Choice:

Unlocking Europe's AI and Innovation Leadership

By **Matthias Bauer, Andrea Dugo** *and* **Dyuti Pandya**,
Director, Economist and Analyst at ECIPE respectively.

EXECUTIVE SUMMARY

Cloud computing underpins digital transformation and is essential for unlocking the benefits of artificial intelligence (AI), automation, and scalable digital services. Yet Europe continues to lag behind global peers in both cloud and AI adoption. This underperformance is not merely technological; it is structural and it is costly. Without rapid progress, the EU risks missing out on over EUR 1.2 trillion in GDP gains across the private sector by around 2030. In the public sector alone, a shift to cloud particularly via a multi-cloud-first strategy could generate up to EUR 450 billion annually in efficiency and productivity gains across EU governments.

A major, yet under-recognised barrier is the lack of cloud customer choice, the ability for businesses and public sector users to freely select, combine, and switch between cloud services. Without this, users face high switching costs, vendor lock-in, and reduced capacity to scale or integrate AI tools effectively.

This paper asks: What are the main obstacles to cloud customer choice in the EU and what are the best avenues for advancing it? The analysis focuses on three key domains that shape the market at large – regulation, competition policy, and standard-setting bodies – examining how each can promote broader customer choice rather than be used narrowly to target individual, innovation-driven firms.

Policy Recommendations: A Dual Strategy for Advancing Cloud Customer Choice

To unlock the full benefits of digital transformation, Europe needs a dual-track strategy – combining quick wins with long-term reform:

1. Short-Term Opportunities

Targeted actions to reduce friction, clarify rules, and support cooperation:

- **For Competition Authorities:** Step up case-by-case enforcement against lock-in practices that fall outside the DMA, including bundling and discriminatory licensing. To avoid legal overlap, ensure a clear separation between DMA enforcement and traditional competition law. Provide practical guidance on when API or architecture alignment is pro-competitive – supporting interoperability, switching, and the EU's simplification goals.
- **For Standard-Setters:** Accelerate practical standards (e.g. via CWAs or ISO PAS), build formal ties with open-source communities, and issue FRAND guidance that distinguishes between service types to reduce uncertainty.
- **For Regulators and Governments:** Use procurement to demand multi-cloud compatibility and open licensing. Support SME participation in standardisation bodies, and issue practical guidance on fair contract terms to reduce legal ambiguity.

2. Long-Term Necessities

Structural reforms to align regulation and standardisation with openness and competition:

- **For Competition Authorities:** Continue to monitor systemic lock-in, while ensuring enforcement supports both proprietary and open-source innovation. Create legal certainty for pro-competitive cooperation on standards.
- **For Standard-Setters:** Institutionalise FRAND practices in governance frameworks and ensure alignment with global initiatives to promote interoperability and cross-border technology diffusion.
- **For Regulators and Governments:** Reform digital regulations to target real harms, not architectures. Redefine sovereignty as user freedom, not supplier nationality. Modernise public procurement to support multi-cloud-by-default – a shift that could unlock up to EUR 450 billion in annual public sector savings and productivity gains.

1. INTRODUCTION

The global data economy is evolving rapidly. As artificial intelligence (AI), cloud computing, and data analytics technologies become more advanced, organisations are gaining access to new tools that enable them to operate more efficiently, deliver higher-value services, and innovate at scale. These developments present major opportunities for private enterprises and the public sector. Moreover, they can improve broader economic resilience and the productivity of entire economies.

However, the structure of cloud and data services markets is also becoming more complex. Cloud platforms are central to the deployment of AI workloads and large-scale data processing, and user needs are diverging in fact, increasingly so. While some organisations continue to rely on general-purpose cloud offerings, others are building specialised data architectures that mix public cloud, on-premise capacity, and third-party services. This specialisation will continue to intensify as technology, service offerings, needs, and security concerns are changing and prompting greater divergence between users simultaneously. For data developments within organisations, there is no "one ring to rule them all". With AI, XG, and quantum technology, the data economy will get even more diffused and decentralised.

Europe, on average, continues to lag behind global peers in cloud adoption particularly in terms of large-scale integration in both the public and private sectors. Several EU Member States are already operating at the global frontier, demonstrating the economic gains that deeper uptake can bring. These disparities suggest that it is not a lack of capacity or potential that holds Europe back, but a failure to accelerate market conditions conducive to greater adoption and innovation. Ensuring that European users can access a wider range of interoperable and competitive services is therefore essential.

In this context, **cloud customer choice emerges** as a key public policy priority. It refers to the ability of cloud and AI service users, whether public or private to select, combine, and switch providers and deployment models according to their operational, compliance, and strategic needs. While not every user requires a multi-cloud or hybrid-cloud solution, the flexibility to design such arrangements is increasingly important, especially as data architectures grow in scale and complexity. Customers making major investments in AI, data management, or cloud-based services need opportunities to contract flexibly and maintain options – avoiding that they will be locked into a single provider with inflexible technical or contractual arrangements. Cloud customer choice can help promote system operability, preserve user bargaining power, and enable tailored solutions across a more diverse cloud services market.

Importantly, cloud customer choice is not the only pathway to user flexibility, but it is an important one that also provides policy makers with agency and actionable ideas. Enhancing it aligns with wider policy objectives around competition, innovation, and market access. It also provides a practical lens through which to examine whether current policy tools are fit for purpose as markets evolve.

This paper asks: What are the main obstacles to cloud customer choice in the EU and what are the best avenues for advancing it? Following a Request for Proposals, the study was commissioned by the Open Cloud Coalition to review barriers to cloud customer choice and greater interoperability in the EU cloud market.

We assess three broad domains that may both provide obstacles and opportunities to cloud customer choice. We analyse their existing and potential role in the market, and not just how they can be used opportunistically to target specific companies.

1. **Regulation** – which has played both helpful and harmful roles in shaping market operability. While EU regulations such as the Data Act, Digital Markets Act, and others introduce broad industry standards, they also raise compliance challenges and technical ambiguities that may hinder cloud customer choice if not carefully implemented.

2. **Competition policy** – which is increasingly focused on the cloud market, especially regarding restrictive licensing practices, bundling, and potential foreclosure. While competition authorities play an important role in ensuring fair market conditions, enforcement remains reactive – bound by procedural limitations, economic rights, and the rule of law – and cannot on its own deliver systemic improvements in market flexibility and architecture.

3. **Standard-setting and FRAND-based frameworks** – which represent a more proactive and adaptable approach. Progress can be made by encouraging industry to develop practical standards, based on clear definitions and a shared understanding of how the market should work. Principles like fair and non-discriminatory access to services can help shape competition policy and guide future regulations, without locking in rigid rules.

Analysing these three opportunities or hinders to cloud customer choice, this study contributes to the important debate on how Europe can build a more open, competitive, and innovation-friendly cloud and AI ecosystem – one that reflects user needs and strengthens the EU's position in the global data economy.

The paper is structured as follows: **Section 2** assesses the current state of cloud adoption across the EU and quantifies the GDP gains from greater use of cloud and AI technologies. It highlights the economic potential of "thick adoption" – the deep, strategic integration of cloud and AI across sectors. **Section 3** examines how existing and proposed EU regulations (Data Act, DMA, DSA, CAIDA and DNA) can hinder interoperability, impose compliance burdens, and reduce switching effectiveness. **Section 4** analyses structural competition barriers in the EU cloud market, such as vendor lock-in, discriminatory licensing, and limited access for smaller providers. **Section 5** argues for open, industry-led standardisation to promote interoperability and customer choice, drawing lessons from other sectors. **Section 6** offers targeted policy recommendations for EU institutions, standard-setters, and competition authorities.

2. UNLOCKING PRODUCTIVITY AND GROWTH: THE ECONOMICS CLOUD AND AI ADOPTION IN EUROPE

2.1 Diagnosing Europe's Cloud Adoption Gap

Despite high ambitions and strong performers like Finland and Denmark, Europe lags behind global peers in cloud computing. This underperformance limits not only efficiency gains but also hampers AI deployment, public service modernisation, and Europe's broader digital competitiveness.

The gap is structural – driven by variation across countries, sectors, and firm sizes. EU adoption remains far below that of the US, Australia, and even emerging markets like Colombia.[1] Public sector uptake is uneven: while Denmark and Estonia lead, others such as France and Germany remain cautious, citing sovereignty concerns.[2] Without targeted action, the EU could forgo up to EUR 450 billion in productivity and cost-saving gains from cloud and AI adoption.[3]

Private sector adoption is similarly slow. As of 2023, only 45.2% of EU firms used cloud services – well below the OECD average. Adoption varies widely across Member States, with Finland leading and countries like Greece, Romania, and Bulgaria trailing significantly. Even Germany and France underperform relative to their economic size.[4] These disparities are detailed in Annex I.

Sectoral and firm-size differences further explain the gap. EU SMEs and traditional industries such as construction, transport, and manufacturing face more barriers to adoption than their counterparts in other advanced economies. Annex I, Table 10 and Table 11 provide a breakdown by sector and firm size.

This lag in cloud uptake has broader implications. Cloud infrastructure is a key enabler of AI deployment, especially for firms that cannot build systems in-house. As AI applications become more data-intensive and compute-hungry, scalable access through cloud platforms becomes essential.

A clear link exists: countries with higher cloud uptake also lead in AI adoption. As shown in Figure 3, digital frontrunners like Finland, Sweden, and Denmark are ahead on both fronts, while France and Spain trail. Failing to invest in cloud adoption means forfeiting leadership in AI – one of the defining drivers of future growth.

---

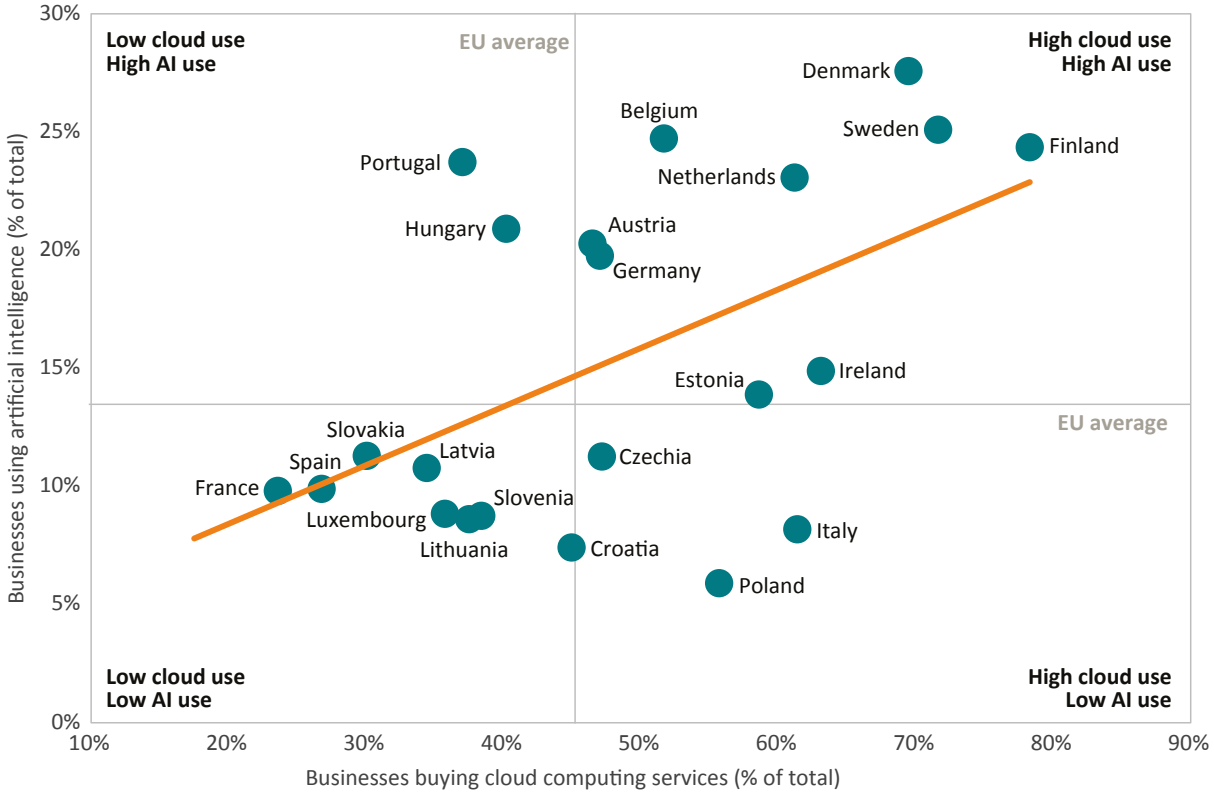
[1] The MIT Global Cloud Ecosystem Index assesses national readiness for cloud adoption by benchmarking countries across four pillars: digital infrastructure, cybersecurity and regulatory assurance, human capital, and industry application. It serves as a comparative tool for evaluating cloud competitiveness in the global economy. See MIT Technology Review (2022) Global Cloud Ecosystem Index 2022. Available at https://www.technologyreview.com/2022/04/25/1051115/global-cloud-ecosystem-index-2022/.

[2] According to a recent study, cloud uptake in the Nordic private sector has added 0.2% to national GDP and created tens of thousands of jobs – particularly in young, innovative firms. Copenhagen Economics (2023). The Economic Benefits of the Cloud in Denmark, Finland and Norway. Available at https://copenhageneconomics.com/publication/the-economic-impact-of-aws-services-in-denmark-finland-and-norway/.

[3] ECIPE (2025). Boosting Efficiency and Quality in EU Public Services: The Need for a European Multi- Cloud-First Strategy. Available at https://ecipe.org/wp-content/uploads/2025/03/ECI_OccasionalPaper_04-2025_LY04.pdf.

[4] Eurostat. (2023, December). Cloud computing - statistics on the use by enterprises. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises.

FIGURE 1: RELATIONSHIP BETWEEN BUSINESS CLOUD SERVICE ADOPTION AND ARTIFICIAL INTELLIGENCE USE AMONG EU-27 MEMBER STATES, 2024 OR LATEST AVAILABLE YEAR (PERCENTAGE OF ALL BUSINESSES)



Source: ECIPE elaboration based on Eurostat and OECD[5] data. Note: The chart includes all available EU-27 Member States, excluding Bulgaria, Croatia, Cyprus, Malta, and Romania, for which data on AI usage is unavailable. The notion of "all businesses" refers to firms with 10 or more employees, excluding those in the financial sector.

2.2 Projecting Growth: Scenarios for Cloud and AI Uptake

As outlined above, the root causes of Europe's lag are largely structural: a high share of SMEs, lower digital maturity in key sectors, and fragmented markets. Unlike the US and China, the EU lacks large-scale cloud demand drivers. This makes supportive policy especially to expand customer choice and interoperability essential for catching up and unlocking the full potential of digital transformation.

[5] OECD. (2024). Businesses using artificial intelligence (AI) (%). Available at https://data-explorer.oecd.org/vis?lc=en&df%5bds%5d=dsDisseminateFinalDMZ&df%5bid%5d=DSD_ICT_B%40DF_BUSINESSES&df%5bag%5d=OECD.STI.DEP&df%5bvs%5d=1.0&av=true&pd=2022%2C2024&dq=.A.G14_B.PT_ENT._T.S_GE10&to%5bTIME_PERIOD%5d=false&vw=tb.

This section explores the macroeconomic impact of increasing adoption under two stylised scenarios. The methodology applied is detailed in Annex II, while the discussion of results is presented in Annex III.

- **Scenario 1 – Ambitious:** All countries reach the current EU leader's adoption levels by sector;
- **Scenario 2 – Less Ambitious:** Countries close half the gap toward those levels.

Customer choice does not itself drive adoption, but it plays a crucial enabling role. The ability to select, combine, and switch providers supports cost efficiency, reduces lock-in, and facilitates integration of increasingly complex AI systems. These dynamics matter especially for SMEs and public authorities with limited capacity for in-house development.

Under Scenario 1, the EU27 could see a 7.3% GDP uplift (EUR 1.2 trillion) over six years. Gains are most pronounced in Member States with currently low adoption levels – notably Romania (+32.4%), Bulgaria (+22.8%), and Poland (+20.8%) – reflecting their strong convergence potential. In contrast, frontrunners like Denmark (+1.6%), Finland (+1.8%), and Sweden (+2.0%) show more modest growth, as much of their digital transition is already underway. Scenario 2 yields a lower projected gain of 4% EU-wide, reflecting slower catch-up. Full results are presented in Annex II.

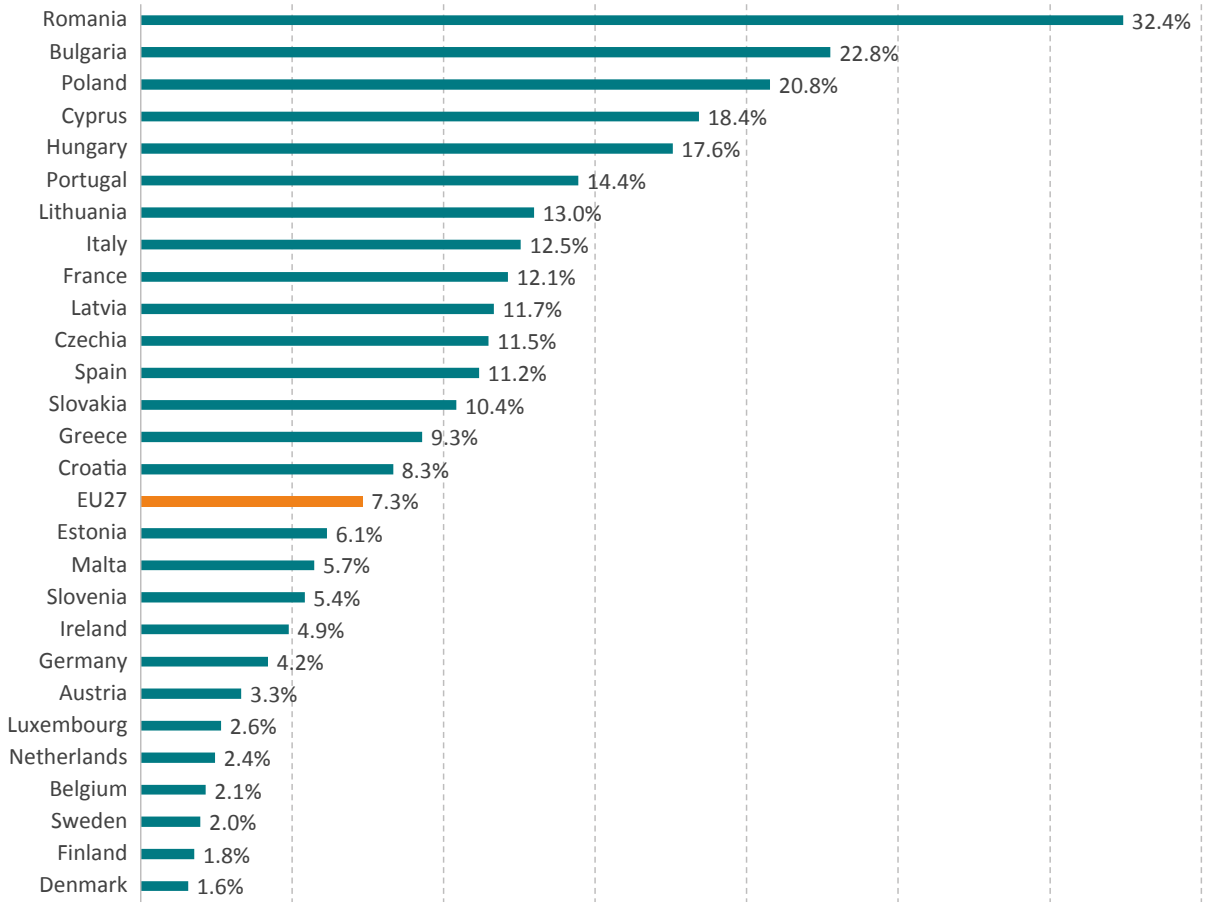
Importantly, these figures should be interpreted as indicative. For countries starting from a very low base, e.g., Portugal, Hungary, Cyprus, Poland, Bulgaria, and Romania, projected gains may appear unrealistically high within a six-year horizon. However, the fundamental point holds: there is massive room for productivity enhancement – not only in the private sector, but particularly in the public sector, where cloud and AI remain significantly underused. Methodological considerations regarding the interpretation and robustness of estimated impacts are provided in Annex III.[6]

Realising these gains depends on more than adoption rates. Deep, transformative ("thick") adoption – where cloud and AI are integrated into core operations – requires modern procurement practices, better interoperability, digital skills, and above all, cloud customer choice. Without these enablers, Europe risks remaining stuck in a phase of shallow, siloed adoption limiting the economic potential of its digital investments.

Figure 2 illustrates GDP gains under Scenario 1. Additional data and methodological notes are included in Annex I.

[6] This assessment estimates potential GDP gains from increased cloud and AI adoption using a structured model based on sectoral GVA and adoption elasticities from empirical studies. It distinguishes between one-off cloud efficiency gains and compounding AI productivity effects. While directionally robust, results are indicative only. They assume convergence to current EU leader benchmarks, apply generalised elasticities, and do not account for adoption depth, transition costs, or second-order effects. Gains may appear high in lagging countries over a six-year horizon, but reflect significant untapped potential especially in the public sector. See Annex III for full methodology and limitations.

FIGURE 2: CHANGES IN GDP – SCENARIO 1 – AMBITIOUS CLOUD AND AI ADOPTION, LONG-TERM (6Y)



Source: ECIPE estimation.

2.3 Modernising Government: The Economic Imperative for Public Sector Cloud Adoption

Public sector cloud adoption in the EU remains limited, particularly at regional and local levels. Many institutions still depend on fragmented, outdated IT systems that are costly to maintain and poorly suited to modern service needs. This hampers not only efficiency and resilience but also the digital responsiveness that citizens increasingly expect.[7]

At the heart of the problem is a lack of cloud customer choice. Without the ability to freely select, combine, and switch between cloud providers, public bodies face vendor lock-in, rigid procurement pathways, and insufficient flexibility to scale modern services. In this context, a multi-cloud-first strategy built on customer choice is essential. It enables institutions to tailor cloud configurations to their operational, security, and compliance needs, fostering competition, improving service quality, and reducing dependency on any single vendor.

[7] ECIPE (2025). Boosting Efficiency and Quality in EU Public Services: The Need for a European Multi-Cloud-First Strategy. Available at https://ecipe.org/wp-content/uploads/2025/03/ECI_OccasionalPaper_04-2025_LY04.pdf.

Where this approach has been implemented, the benefits are clear. Finland uses Oracle and Microsoft for claims and payment systems; Spain has integrated emergency services through Hexagon; and Italy enables cross-regional health data exchange on AWS. These examples show that even sensitive domains can adopt cloud at scale – but only where trust, legal clarity, and choice enable it.

However, such cases remain the exception. Without real customer choice, multi-cloud remains a slogan, not a strategy. Uptake is slowed by rigid procurement rules, fragmented governance, and institutional risk aversion. Broader adoption could unlock up to EUR 450 billion annually in cost savings and productivity gains across EU governments through better resource allocation, faster service delivery, and improved data sharing. But this potential depends on modern, open cloud markets where public institutions are free to design the systems they need.[8]

Estonia shows what is possible. Its e-government model underpinned by the X-Road data exchange and a single digital ID has delivered near-universal digital access and productivity gains worth approximately 2% of GDP annually. Critically, its success is built on interoperability, procurement agility, and infrastructure designed with customer choice in mind.

For Europe to follow suit, cloud customer choice must become a cornerstone of public sector digital policy. A multi-cloud-first approach without real choice is an empty promise. Yet where choice is guaranteed, governments can avoid lock-in, design citizen-centric platforms, and future-proof their digital infrastructure. To lead by example, EU and national authorities must align procurement frameworks with interoperability goals and remove structural barriers to flexible cloud adoption. Public sector leadership in this area can accelerate digital transformation across the economy.

3. POLICY AND REGULATORY BARRIERS TO CLOUD CUSTOMER CHOICE

Cloud computing is no longer confined to virtualised resources in distant data centres. It is rapidly evolving into a decentralised, intelligent infrastructure merging with AI and next-generation networks like 5G and 6G.[9] While cloud infrastructure remains vital for storage and analytics, edge computing enables real-time decisions by processing data at the source. AI bridges the two, learning centrally and acting locally. As adoption deepens, success will depend on new

[8] Ibid.

[9] For example, the 2024 the Body of European Regulators for Electronic Communications (BEREC) Report on Cloud and Edge Computing Services confirms that cloud computing is undergoing a fundamental shift from centralised data centre models to decentralised, intelligent infrastructures. This transition is driven by the convergence of cloud with AI, edge computing, and next-generation networks such as 5G and 6G. BEREC notes that by 2025, up to 80% of data is expected to be processed closer to the user, highlighting the strategic role of edge nodes. This transformation supports the EU Digital Decade 2030 objectives, which call for 75% of businesses to adopt cloud-edge technologies and for the deployment of 10,000 climate-neutral edge nodes. The BEREC report also stresses the need for regulatory coherence to address market concentration, promote interoperability, and support innovation in an increasingly hybrid digital infrastructure. See BEREC (2024). BEREC Report on Cloud and Edge Computing Services. Available at https://www.berec.europa.eu/system/files/2024-03/BoR%20%2824%29%2052_Draft_Cloud_Report.pdf.

standards, robust data governance, and sustainable infrastructure. This transition promises a more responsive, personalised, and resilient digital economy.[10]

As cloud, edge, AI, and connectivity infrastructures increasingly converge, traditional service layer distinctions such as IaaS, PaaS, and SaaS are becoming less clear-cut, and arguably less meaningful. Yet, since the adoption of the EU's data strategy policy efforts at the European level have increasingly promoted data portability and switching.[11] In response, cloud computing has become a focus area for introducing binding legal obligations on service providers, particularly to strengthen data portability and service interoperability.

Key regulatory actions include the Data Act (DA)[12], which aims to improve switching and interoperability between cloud, edge, and other data processing services; the Digital Markets Act (DMA)[13], which aims to addresses fairness and contestability in core platform services, including cloud; and the Digital Services Act (DSA),[14] which aims to classify cloud services as part of hosting services. In addition to these measures, the proposed Digital Networks Act (DNA) could significantly expand telecom-style regulation to cloud infrastructure, raising concerns about legal overreach and inappropriate regulatory analogies. Furthermore, the proposed Cloud and AI Development Act seeks to promote Europe's digital competitiveness but may introduce overlapping compliance obligations that risk complicating the regulatory environment for cloud and AI providers. [15]

This regulatory pacing problem, the mismatch between fast-moving technologies and slower, often reactive regulatory frameworks creates friction and hinders interoperability. Without a policy framework that encourages technological and market development, many new regulations will constrain cloud deployment models and new competition between established or new companies. Uncoordinated and overly prescriptive regulations that work with old categories of data and services will eventually hinder a market that already moves toward multi-cloud adoption and greater interoperability.

In this environment, regulations should promote the availability of diverse service and technology models, reflecting the varied needs and preferences of customers who face significant investment costs to adopt new technologies and drive organisational change. Cloud customer choice is emerging as a key guiding principle in the evolving cloud and AI markets. However, several EU regulatory and policy initiatives risk undermining this principle by creating legal uncertainty, imposing technical requirements without sufficient feasibility assessments, or failing to reflect

[10] European Commission (2024). Edge Observatory 4 Deployment Data Report from 2024. Available at https://digital-strategy.ec.europa.eu/en/policies/cloud-computing. Also see European Commission (2019). Cloud and Edge Computing: a different way of using IT — Brochure. Available at https://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-it-brochure.

[11] European Commission (2025). European data strategy. Available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

[12] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[13] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[14] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[15] European Commission (2024). White Paper - How to master Europe's digital infrastructure needs? Available at https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs. European Commission (2025). AI Continent – new cloud and AI development act. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act_en.

the integrated nature of cloud markets. This section identifies and critically assesses the most significant regulatory and policy barriers to market choice, diversity, and cloud customer choice in the EU.

3.1 The Data Act: From Interoperability to Overreach

The Data Act seeks to enable greater user mobility and competition in cloud markets through switching and interoperability obligations. However, several provisions apply undifferentiated rules across diverse market segments and technical environments. This section outlines five regulatory misalignments that, in practice, risk constraining rather than improving cloud customer choice.

The regulatory issues identified in Table 1 highlight how several provisions of the Data Act, though well-intentioned, risk undermining the very goals they aim to achieve. By applying uniform rules across a complex and layered cloud services market, the Act fails to account for key differences in market structure, technical design, and user needs. The following discussion outlines each concern in more detail, showing how regulatory ambiguity, misaligned incentives, and technical infeasibility could limit service diversity, stifle innovation, and ultimately reduce effective cloud customer choice.

TABLE 1: EU DATA ACT: KEY REGULATORY ISSUES AND IMPLICATIONS FOR CLOUD CUSTOMER CHOICE

Regulatory Issue	Description	Implications for cloud customer choice
1. Overgeneralised Market Diagnosis	DA imposes symmetric obligations across IaaS, PaaS, and SaaS despite different market dynamics and switching costs.	Over-regulation of competitive segments; reduced service innovation.
2. Ambiguity in "Same Service Type"	Vague definitions conflate substitutable and complementary services.	Compliance uncertainty; disincentive for integrated solutions.
3. Unclear Unbundling Mandates	Obligations apply to technically integrated or bespoke services without feasibility checks.	Fragmented service architectures; degraded performance.
4. Functional Equivalence Requirements	DA mandates service continuity without clear technical standards or flexibility.	Legal uncertainty; convergence around lowest common denominators.
5. Switching Cost Restrictions	While a blanket ban on switching fees increases pricing transparency and may benefit smaller providers by reducing artificial barriers to customer switching. However, it may also prevent cost-reflective compensation for genuine switching-related expenses, particularly in complex infrastructure settings.	Can support portability and encourage competition, but risks unintended effects if smaller providers cannot recover switching-related costs, potentially affecting service quality or customisation options.

Source: ECIPE compilation.

Individually, these issues raise costs and risks for service providers. Collectively, they can discourage innovation and reduce service differentiation in the EU and limit the practical value of switching rights. By applying one-size-fits-all obligations, the Data Act fails to accommodate the layered nature of cloud markets and the technical realities of integration, customisation, and infrastructure constraints.

Cloud customer choice depends on more than the legal right to switch. It requires a diverse, competitive ecosystem where providers can develop tailored offerings, and users can make informed decisions based on performance, price, and interoperability. Without clear distinctions between service types, realistic provisions for integrated solutions, and flexibility for market-driven technical standards, the Data Act may unintentionally reinforce market concentration by disadvantaging smaller or more innovative players.

In short, the current regulatory model risks formalising ("notional") portability without enabling it in practice. A more targeted, technically grounded approach is needed to realise the DA's goal of a more open and user-friendly cloud market.

3.1.1 Principal Regulatory Shortcomings of the Data Act

Each of the following provisions introduces specific challenges:

1. **Overgeneralised Market Diagnosis:** The Data Act applies the same obligations to IaaS, PaaS, and SaaS, overlooking the fact that while IaaS markets are concentrated, the upper layers are more dynamic and diverse. This approach risks over-regulating segments where switching barriers are already lower and innovation is frequent.

2. **Ambiguity in "Same Service Type"**: The current definition groups services based on broad similarities in function, ignoring significant differences in processing models and use cases.[16] This could lead to inappropriate application of switching rules to services that are complementary rather than substitutable.[17]

3. **Unclear Unbundling Mandates:** Article 23(e) appears to require unbundling of services even where tightly integrated technical architectures or bespoke configurations make this impractical. While Article 31 offers some exemptions, the lack of clear alignment generates legal uncertainty and risks enforcement inconsistencies.

[16] Areas of the cloud market such as accounting software, productivity suites, customer relationship management (CRM) systems, and application development platforms, where numerous providers compete on features, pricing, and usability. These segments are typically characterised by high innovation, low switching costs, and frequent user substitution. Businesses often migrate between tools without major technical or contractual barriers. Imposing uniform switching obligations in these flexible markets risks overregulating competitive ecosystems and placing unnecessary burdens on smaller or specialised providers. See, OECD (2025). Competition in the provision of cloud computing services. Available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf.

[17] Ennis, S. F., & Evans, B. (2023). Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence. Available at https://ssrn.com/abstract=4395183https://ssrn.com/abstract=4395183. Also see Manganelli, A. and Schnurr, D. (2024). Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies. CERRE. Available at: https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf.

4. **Functional Equivalence Requirements:** Articles 2(37) and 30(2) necessitate providers to preserve functionality when switching occurs, but without clear standards, this could lead to unpredictable interpretations and compliance disputes. Providers may respond by simplifying or homogenising their services to reduce legal risk.

5. **Switching Cost Restrictions:** Article 29 prohibits switching fees, but fails to distinguish between unfair lock-in charges and legitimate cost recovery. Smaller providers may be forced to internalise migration expenses, distorting price signals and reducing service transparency for users.

3.1.2 Bundling, Unbundling, and Licensing Barriers

The Data Act's approach to bundling and licensing creates legal and practical challenges that may undermine cloud customer choice. Bundled services such as integrated SaaS platforms combining HR, finance, and procurement tools often offer performance, security, and usability advantages. Yet Article 23(e) introduces an unbundling obligation that may force separation of services, even when technically integrated or bespoke. Article 31 provides exemptions for custom-built offerings, but it does not explicitly cover Article 23(e), creating legal ambiguity. This gap means services excluded from other switching duties under Articles 23(d), 29, and 30 may still face unbundling obligations, despite being unsuitable for disaggregation. Clarifying the alignment between Article 23 and Article 31 would reduce compliance uncertainty and enforcement risk.

In practice, technically separating integrated services is not always feasible. Many providers rely on proprietary architectures or internal APIs, and widespread adoption of open standards as encouraged by Article 30 remains limited. Mandating unbundling without considering technical realities may degrade service quality and increase costs. For instance, a public agency wishing to replace only the payroll module of an integrated suite may face reengineering efforts that outweigh the benefits of partial switching.

At the same time, licensing and pricing practices also play a critical role in shaping user lock-in. The Data Act currently lacks provisions to support the portability of on-premise licences to cloud environments, or their use across multiple providers – a key requirement for multi-cloud strategies. Enterprises that wish to avoid dependency on a single vendor are often constrained by licence terms that restrict flexibility or impose cost penalties.

Investigations such as those by the UK's CMA (also see Section 4) have drawn attention to licensing models that could entrench incumbency and discourage competition. Without regulatory scrutiny, restrictive licence conditions can offset the gains of technical portability by making it economically unviable to switch or multi-source services.

To address these gaps, licensing transparency and portability could become a policy priority. Public procurement rules in particular can incentivise licence models that promote interoperability, switching, and multi-cloud compatibility. In combination with more standardised

technical reforms (see Section 5), such steps are essential to ensuring that portability rights translate into real market options.

3.2 The Digital Markets Act (DMA): Misalignment with Cloud Market Realities

While the Digital Markets Act (DMA) aims to improve fairness and contestability in digital markets, its inclusion of cloud services as Core Platform Services (CPSs) introduces significant conceptual and practical ambiguities (Article 3). The DMA's regulatory logic is grounded in concerns over market dynamics typical of multi-sided platforms such as search engines and app stores where network effects, data-driven advantages, and platform intermediation raise risks of dependency and lock-in. However, cloud services, especially IaaS and PaaS operate primarily as one-sided business models, offering infrastructure to enterprise clients rather than acting as intermediaries between user groups. This divergence is reflected in Articles 5 and 6, where obligations are unevenly distributed across CPSs operating under fundamentally different business models.[18]

As the scope of the DMA expands to cover a diverse set of services and markets, harmonising ex-ante obligations becomes increasingly complex. Ultimately, "digital markets" do not constitute a single industry, but rather span across multiple sectors, making one-size-fits-all regulation potentially problematic.

3.2.1 Ambiguity in Business User Classification

A complication in applying the DMA to cloud services is the broad and imprecise definition of a "business user", any natural or legal person acting in a commercial capacity to offer goods or services to end users via the core platform service. In the context of cloud services, particularly IaaS and PaaS, this definition is problematic. Most cloud customers use these services to support internal operations, not to deliver end-user-facing products via the platform itself. As such, the DMA's user-based thresholds for designating gatekeepers may misrepresent market dynamics in cloud markets, where large user bases do not necessarily imply dependency or control.

Moreover, the DMA's implicit assumption that user scale equates to market dominance fails to account for the contestability of cloud markets. Despite concentration at the infrastructure layer, innovation is rapid, switching costs can be managed through multi-cloud and containerisation strategies, and new entrants continue to compete successfully in niche or high-performance segments. Competitive pressures from new entrants, smaller providers, and evolving customer demands continually disrupt the cloud services market. In response, cloud providers are driven to innovate by adopting emerging technologies such as edge computing, hybrid cloud architectures, and AI-powered services to maintain strategic advantage.[19] Relying on simplistic numerical thresholds risks overstating market power and misdirecting regulatory scrutiny.

---

[18] Manganelli, A. and Schnurr, D. (2024). Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies. CERRE. Available at: https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf.

[19] OECD. Oligopoly Markets' Available at: www.oecd.org/daf/competition/oligopoly-markets.htm.

Implications for cloud customer choice:

Misclassifying cloud customers as "business users" risks triggering gatekeeper obligations that are poorly aligned with the nature of cloud services. For providers, this could lead to over-compliance, reduced investment in specialised offerings, and a retreat from high-value services that do not scale broadly. Consider a cloud vendor offering bespoke infrastructure solutions for financial institutions or research organisations might exceed the DMA's business user threshold, despite operating in a highly tailored, low-volume segment with no meaningful gatekeeping power. Faced with gatekeeper designation, such providers could scale back or discontinue these niche services to avoid regulatory exposure. For users, regulatory uncertainty erodes transparency, complicates comparisons, and reduces confidence in switching providers. The result is a less dynamic and more constrained cloud market, where customer choice is narrowed not by technical limitations, but by legal ambiguity.

3.2.2 Misfit with Intermediation Logic

The DMA targets platforms that serve as intermediaries between business users and end consumers, imposing obligations intended to curb abuses of data access, self-preferencing, and gatekeeping in multi-sided markets. However, many cloud providers, particularly those offering IaaS and PaaS, do not function as intermediaries. They primarily deliver backend infrastructure or development environments that are consumed directly by businesses, with no facilitation of downstream, consumer-facing interactions.

This intermediary logic is reflected in Article 6(2) of the DMA, which prohibits gatekeepers from using non-public data provided by business users to compete against them. The assumption here is that platforms have visibility into user operations, which may be true for cloud marketplaces, where providers mediate listings, transactions, or analytics. However, in IaaS models, such visibility is typically absent as providers supply compute capacity rather than mediate business relationships. Applying Article 6(2) too broadly could thus conflate distinct business models and lead to overregulation in areas where competitive harm is unlikely.

Article 6(7) mandates interoperability with third-party software and hardware, which could disrupt the customisation and security architectures vital to enterprise cloud environments. Article 6(9) requires real-time access and portability of end-user data, yet in IaaS/PaaS models, such data may not even be visible to the provider, making the obligation technically and legally ambiguous.

Implications for cloud customer choice:

In this capacity, the DMA functions as a new institutional mechanism that performs critical market governance functions: selecting which platforms warrant special oversight, allocating rights and responsibilities among market participants, and providing information that guides market behaviour and expectations.[20] However, when regulatory obligations are misaligned with platform function or market structure, they may reduce the availability of differentiated offerings and

[20] Manganelli A., Nicita A. (2022) Regulating digital markets: the EU Approach. Palgrave.

discourage providers from developing specialised or scalable solutions. Consider, if obligations under the DMA such as real-time data access for business users or prohibitions on self-preferencing were applied to IaaS providers offering GPU-as-a-service, they could be forced to disclose sensitive system telemetry or adjust performance configurations in ways that undermine their core business model. Unlike platforms that mediate transactions or content between third parties, these services are not intermediaries but infrastructure enablers. Imposing the wrong rules increases compliance burdens, weakens service differentiation, and ultimately narrows the options available to customers seeking tailored or high-performance solutions.

These issues underscore the complexity of using the DMA to address unfair practices in the cloud sector. Doing so would likely require targeted amendments to existing obligations to make them applicable to cloud services and parallel adjustments to prevent unintended consequences that could stifle innovation or impair service quality.

3.3 The Digital Services Act (DSA): Misclassification, Risks and Compliance Overreach in the Cloud Context

The Digital Services Act (DSA) establishes horizontal rules for online intermediaries with the goal of improving safety, transparency, and accountability in the digital environment. While its framework may be well-suited to consumer-facing platforms that host and disseminate user-generated content, its application to enterprise cloud computing raises serious concerns. By categorising cloud services particularly IaaS and PaaS as generic "hosting services", the DSA risks imposing ill-fitting obligations on providers that do not function as content intermediaries. The result is a regulatory misalignment that could generate legal ambiguity, inflate compliance burdens, and restrict service availability, all of which threaten to weaken cloud customer choice across the EU.

3.3.1 Classification as Hosting Services

Under Article 2(1), hosting services are defined as those that store data and make it available at the request of a recipient. This broad definition already fails to distinguish between consumer-facing online platforms and enterprise-grade cloud infrastructure. As a result, obligations designed for platforms disseminating public content such as notice-and-action requirements for illegal material risk being misapplied to cloud services that support private, internal enterprise operations. Enterprise-oriented cloud services are typically used for secure storage and processing of confidential business information, including internal databases, encrypted backups, and proprietary applications. Providers of these services usually have neither access to nor control over the content stored by clients. Applying public content moderation duties to such environments is not only technically infeasible but also misaligned with the nature of the service.

Implications for cloud customer choice:

Misclassifying enterprise cloud infrastructure services as public-facing hosts under the DSA could expose providers to inappropriate liability frameworks and disproportionate compliance

obligations. The term "public" is not explicitly defined in the DSA,[21] which creates ambiguity around whether content stored on cloud platforms, regardless of its visibility or intended audience, might trigger obligations typically reserved for platforms that host user-generated content for public access. If interpreted broadly, such a classification could impose burdensome responsibilities, such as content moderation or notice-and-action procedures, on providers who neither control nor monitor the content hosted by their business clients. This misalignment between the DSA's obligations and the actual function of cloud infrastructure services highlights the need for a more tailored regulatory approach. While the DSA rightly seeks to promote a safer online environment, it must also ensure that obligations are proportionate and aligned with the technical and operational realities of different types of intermediary services

Consider providers that support highly sensitive business applications, internal databases, and encrypted customer data, none of which is intended for public dissemination or interaction. Applying Article 16's content removal obligations to such services not only misaligns with their architecture but also exposes them to legal conflict. DSA liability exemptions under Article 6 depend on lacking "actual knowledge" of illegal content, yet these providers are not designed to inspect or monitor such data. Complying with one legal standard may risk violating another, such as GDPR or contractual confidentiality. This regulatory mismatch may discourage providers from offering high-assurance or specialised services in the EU, narrowing market diversity.

3.4 The Proposed Digital Networks Act (DNA) and Cloud Choice

The forthcoming DNA aims to modernise EU connectivity regulation. Yet by blurring the line between telecommunications and cloud services, it risks becoming a major obstacle to cloud customer choice. While 5G and edge computing interface with cloud platforms, these technologies serve distinct functions.[22] Treating cloud services as equivalent to telecom infrastructure, as considered by some policymakers, could lead to disproportionate obligations, stifling innovation and investment at a time when Europe is striving for digital competitiveness.[23]

This regulatory approach also reveals a strategic contradiction. On the one hand, the EU seeks technological sovereignty and global leadership in AI; on the other, it risks undermining the very infrastructure required to support these ambitions. Scalable compute and storage capacities form the backbone of AI development, digital healthcare, and next-generation public services. Overburdening cloud providers with telecom-style regulation would not only affect private operators but could also stall public sector digitisation.

---

[21] Bania, K., & Geradin, D. (2023). The regulation of cloud computing: why the European Union failed to get it right. Information & Communications Technology Law, 33(1), 99–113. https://doi.org/10.1080/13600834.2023.2260687

[22] While the full proposal for the Digital Networks Act (DNA) has not yet been published, concerns can reasonably be raised based on how similar regulatory frameworks have evolved. It is not uncommon for legal or regulatory categories to expand over time, sometimes inappropriately to cover entities, activities, or services that were not originally intended to fall within their scope. In this context, there is a credible risk that the DNA could extend definitions or obligations in ways that inadvertently capture cloud infrastructure providers, imposing requirements that do not align with their technical function or market role. 3GPP (2023). Edge Computing. Available at https://www.3gpp.org/technologies/edge-computing.

[23] See the broad regulatory options outlined in the European Commission's consultation on the proposed Digital Networks Act. European Commission (2025). Call for evidence for an impact assessment - Ares(2025)4545535. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14709-Digital-Networks-Act_en.

3.4.1 Legal Misclassifications

Following the regulatory options outlined by the European Commission, the DNA appears to rest on the assumption that convergence between networks and cloud justifies treating cloud providers more like electronic communications services (ECS).[24] Yet telecoms deliver data transport; cloud providers deliver compute, storage, and application-layer services. These functions differ in technical architecture, user relationships, and economic models. Extending obligations such as service availability guarantees or universal service levies from telecoms to cloud providers would fundamentally alter the legal status of cloud services, transforming them from enterprise software platforms into regulated utilities.

Implications for cloud customer choice

Misclassifying cloud infrastructure services as electronic communications services under the DNA risks subjecting them to obligations designed for telecom networks such as guaranteed service availability, interoperability with unrelated systems, or licensing and access regulation. These requirements are poorly matched to the operational logic of cloud platforms, which are built for flexibility, scalability, and service differentiation. Imposing such telecom-grade compliance standards on cloud providers could increase operational costs, reduce their ability to offer specialised or high-performance services, and discourage investment in tailored infrastructure. This would directly constrain user choice in strategic areas such as AI model training, data-intensive manufacturing systems, and public sector digital transformation, all of which rely on access to configurable, workload-optimised cloud environments.

Consider specialised cloud services such as GPU-accelerated environments for AI training, were reclassified under the proposed DNA as electronic communications services, providers could become subject to telecom-grade obligations designed for connectivity infrastructure rather than computing platforms. These could include stringent availability requirements, resilience standards, or interoperability mandates that are not aligned with the flexible, scalable nature of cloud-based AI services. Such a reclassification would significantly increase compliance costs and operational complexity, particularly for providers offering niche, high-performance environments. Faced with these burdens, some may scale back their European offerings or avoid investing in advanced infrastructure altogether. This would reduce the availability of cutting-edge compute resources for AI developers, manufacturers, and public institutions, thereby weakening Europe's goals for cloud capacity, competitiveness, and digital autonomy.

[24] Ibid.

3.4.2 Outcomes to Avoid

3.4.2.1 Regulatory Fragmentation across Member States

If the DNA were to subject cloud infrastructure services to telecom-style oversight, there is a significant risk of inconsistent interpretation and enforcement across Member States. National regulatory authorities, many of which are traditionally focused on telecommunications, may lack the technical expertise to oversee complex, multi-layered cloud infrastructure. This could result in regulatory divergence, where the same cloud service is subject to different obligations, reporting requirements, or compliance timelines depending on the Member State. For example, if one country's telecom regulator interprets the DNA as requiring full reporting of all service disruptions, while another applies minimal oversight, a provider operating across both jurisdictions would need to implement duplicative compliance systems. This creates operational complexity and legal uncertainty, undermines the Digital Single Market, and discourages providers from offering consistent, pan-European cloud services. For customers, this may translate into fragmented multi-cloud deployments, contractual incompatibility, and reduced access to interoperable, cross-border services.

3.4.2.2 Top-Down Interoperability Mandates

In parallel, the DNA may introduce static, top-down interoperability requirements that do not reflect the architectural diversity or evolving business models of cloud services. While interoperability is essential, imposing uniform technical protocols or fixed APIs risks homogenising the cloud ecosystem, reducing flexibility for providers and users alike. For instance, if the DNA mandates a single set of interoperability standards, a healthcare organisation using a customised AI pipeline across multiple cloud environments could be forced to switch to a generic configuration that meets regulatory requirements but lacks the performance, security, or compliance features tailored to sensitive medical data. This would degrade service quality and limit the ability to adopt best-fit or cutting-edge solutions, narrowing cloud customer choice in critical sectors like health, research, and manufacturing.

3.5 The Proposed Cloud and AI Development Act

The Commission's forthcoming Cloud and AI Development Act (CAIDA) is intended to address the EU's structural shortfall in high-performance computing and sovereign cloud capacity, particularly for large-scale AI model training and deployment. CAIDA is expected to set out measures to mobilise public and private investment, support the development of regionally distributed compute infrastructure, and establish technical and policy frameworks that ensure security, sustainability, and interoperability across AI and cloud systems. In doing so, it will play a critical role in shaping the EU's capacity to compete globally in AI innovation, while reducing reliance on non-European providers and strengthening control over data and infrastructure.

As outlined in the Call for Evidence, CAIDA is likely to combine hard and soft law measures to scale EU-based data centre capacity, boost resource-efficient innovation, and ensure secure cloud options for critical use cases.[25] It is anchored in the logic of the Draghi Report[26], the Competitiveness Compass[27], and EVP Virkkunen's mission letter[28], all of which frame cloud infrastructure as essential to Europe's long-term competitiveness and strategic autonomy. Yet the very ambition of the Act also creates risks: if poorly designed, it could unintentionally reinforce barriers to cloud customer choice, discourage international investment in Europe, or entrench regulatory fragmentation.

At the same time, CAIDA may be an opportunity to tackle issues such as restrictive software licensing. Encouraging licensing practices that facilitate portability and deployment flexibility could help unlock meaningful interoperability, without undermining the diversity of cloud business models.

As the regulatory landscape continues to evolve, upcoming initiatives such as the DNA or revisions to the European Electronic Communications Code (EECC) may further affect cloud infrastructure providers. It is crucial that these frameworks remain clearly delineated from the scope of the proposed CAIDA to avoid overlapping or contradictory obligations – particularly in relation to service classification, incident reporting, and interoperability requirements. The following section outlines key challenges that risk undermining the development of a competitive and innovation-friendly European cloud and AI ecosystem.

1) Capacity Expansion as a Pretext for Market Closure

The EU's ambition to triple data centre capacity is both bold and necessary, yet it raises concerns if interpreted as a mandate to exclude non-EU providers or impose restrictive localisation requirements. With an estimated USD 1.36 trillion investment gap in ICT and cloud infrastructure compared to the US, closing this gap will require access to global capital and capabilities.[29] The concept of "sovereign" infrastructure for critical use cases need not conflict with an open market for general-purpose compute services. Policy choices that prioritise protectionism over openness risk misallocating resources and constraining access to the world's most advanced technologies.

2) Conflating Cloud Services with Telecommunications

The technological convergence of networks, compute, and AI has sparked proposals to regulate cloud services under telecoms frameworks. However, compute services differ significantly from

[25] As with the Digital Networks Act (DNA), the analysis of CAIDA remains necessarily speculative, as the full scope and legal framing of the proposal are not yet known. However, given the tendency of EU digital policy frameworks to evolve through broad, sometimes overlapping regulatory interpretations, it is reasonable to anticipate a range of possible implications depending on how the legislation is ultimately structured and enforced. European Commission (2025). Call for evidence - AI Continent – new cloud and AI development act. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act_en.

[26] European Commission (2024). The future of European competitiveness: Report by Mario Draghi. Available at https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

[27] European Commission (2025). A Competitiveness Compass for the EU. Available at https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en.

[28] European Commission (2024). Henna Virkkunen - Mission letter. Available at https://commission.europa.eu/document/3b537594-9264-4249-a912-5b102b7b49a3_en.

[29] ECIPE (2024). The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities: The Case for a New Approach to Cloud Policy. Available at https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/.

traditional connectivity infrastructure, both in function and business model. Attempts to apply telecom-style obligations through instruments such as the DNA may mischaracterise the nature of cloud markets and inhibit innovation. The Draghi Report instead calls for simplification – notably a "Single Market passporting regime for all EU-provided cloud services" – reflecting the need for more agile and appropriate regulatory approaches.

3) Interoperability: Between Facilitation and Fossilisation

While interoperability is a key enabler of cloud competition and innovation, overly rigid or centralised mandates risk freezing technological development. The experience of initiatives like GAIA-X demonstrates the difficulty of imposing common architectures from the top down, particularly when industry adoption remains limited. Innovation in cloud services is increasingly modular and fast-moving, and regulatory approaches must evolve accordingly – encouraging open processes rather than encoding today's technical solutions into law.

4) Ambiguity in "Critical Use Cases" and Assurance Levels

The Act's focus on securing highly critical use cases raises legitimate concerns about public risk and resilience. Yet without narrowly defined categories and clear thresholds, this concept risks becoming a catch-all justification for restrictive national mandates. Vague definitions also invite divergence across Member States, creating regulatory uncertainty for providers and increasing fragmentation across the Single Market. Previous economic modelling by ECIPE shows that even modest exclusions could carry substantial macroeconomic costs.[30]

5) Overlooking Global Standards and International Supply Chains

Europe's cloud and compute ecosystem is deeply embedded in global value chains. Initiatives that prioritise EU-specific standards over internationally adopted frameworks – such as ISO, IEEE, or open-source foundations like Kubernetes – risk creating redundant or incompatible layers of compliance. Past attempts to assert digital sovereignty through exclusive frameworks (e.g., Gaia-X or national certification schemes) have largely failed to produce competitive alternatives. A more globally aligned approach would better support interoperability, customer choice, and market access.[31]

6) Disincentivising Modularity and Specialisation

Policy frameworks that implicitly favour vertically integrated, full-stack providers risk sidelining the many innovative firms that focus on modular or specialised services – including orchestration, identity management, and sector-specific AI platforms. While initiatives like "EuroStack" may appeal politically, they are unlikely to reflect market realities. Most providers, including those

[30] ECIPE (2023). The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States. Available at https://ecipe.org/publications/eucs-immunity-requirements-economic-impacts/. Also see ITIF (2025). The EU's Cloud Service Restrictions. Available at https://itif.org/publications/2025/05/25/eu-cloud-service-restrictions/.

[31] Calcara (2025). European cloud computing policy: failing in Europe to succeed nationally? Available at https://www.tandfonline.com/doi/full/10.1080/01402382.2025.2491962?src=exp-la.

advocating for European sovereignty, rely on modular technologies sourced globally.[32] The future competitiveness of Europe's cloud sector will depend not on replicating entire stacks, but on fostering interoperability across a diverse set of actors.[33]

7) Fragmented Procurement and Permitting Rules

Legacy procurement and permitting processes remain major barriers to public-sector cloud adoption and infrastructure expansion. National fragmentation not only slows adoption but also hampers multi-cloud uptake and prevents smaller or non-incumbent providers from participating on equal terms. As the Public Procurement Directive is reviewed, there is an opportunity to integrate cloud-specific provisions, reduce administrative burden, and promote fair competition.[34] Without this, the EU risks missing out on the digital transformation gains that more agile and inclusive procurement could unlock.

4. COMPETITION CHALLENGES IN CLOUD MARKETS

Beyond legislative measures, a range of initiatives at both EU and national levels have been launched to scrutinise cloud computing markets and identify competition barriers and market failures. These regulatory efforts intersect with mounting concerns over market dynamics and procurement practices in the cloud sector. A particularly contentious issue involves allegations that some vendors engage in unfair software licensing, charging higher fees when customers run licensed software on rival cloud infrastructure. While such licensing practices are rarely viewed in isolation as the decisive factor in provider selection, they can significantly influence the competitiveness of alternative cloud offerings.

4.1 Competition Authority Concerns with Cloud Competition

Competition authorities have increasingly turned their attention to cloud and data storage services. Across the EU, the UK, and the U.S., regulators are increasingly scrutinising bundling practices, software licensing restrictions, and strategic partnerships in cloud and AI markets, especially involving Microsoft.

In the EU, the European Commission is pursuing several investigations: one triggered by Slack's 2020 complaint against Microsoft for bundling Teams with Office, and another prompted by OVHcloud, Aruba, and the Danish Cloud Community, who allege that Microsoft's licensing terms unfairly penalise customers using non-Azure infrastructure. The Commission is also assessing whether Microsoft's investment in OpenAI could fall under EU Merger Regulation, reflecting broader concerns about vertical integration in the generative AI space. In 2024, the

[32] See, e.g., ECIPE (2025). EuroStack's Hypocrisy: A European Vision Built on American Cloud Solutions? Available at https://ecipe.org/blog/eurostacks-hypocrisy/.

[33] See Section 9.

[34] See, e.g., European Commission (2025). Call for evidence – Public procurement directives – evaluation. Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14427-Public-procurement-directives-evaluation_en.

European Commission also conducted unannounced antitrust inspections targeting the data centre construction sector.[35]

In July 2024, Microsoft and CISPE (the Cloud Infrastructure Services Providers in Europe association, founded in 2016) reached a settlement over a competition complaint CISPE filed with the European Commission in November 2022, alleging unfair software licensing practices. Under the agreement, Microsoft will develop a new version of Azure Stack HCI for European cloud providers, offering features such as multi-session Windows 11 desktops and pay-as-you-go SQL licensing, with a nine-month deadline to deliver. The deal also establishes an independent European Cloud Observatory (ECO) to monitor implementation and ensure fair licensing; in return, CISPE withdrew its complaint and received a lump-sum reimbursement for litigation and campaign costs, but reserved the right to refile if Microsoft fails to meet its commitments.[36]

In the UK, the Competition and Markets Authority (CMA) has launched a series of inquiries into major cloud-AI partnerships. These include Microsoft's deals with OpenAI and Inflection AI, and the relationships between Amazon and Anthropic, as well as Google and Anthropic. These investigations aim to determine whether such arrangements harm market contestability by reinforcing dominant positions in foundational AI technologies and limiting opportunities for rivals to scale. The CMA's proactive stance reflects a wider strategy to address concentration risks early – before they entrench.

In Germany, the Bundeskartellamt has classified Microsoft as a company of "paramount cross-market significance", allowing it to act swiftly against potential anti-competitive behaviour not covered by the EU Digital Markets Act. This includes Microsoft's increasing integration of identity, productivity, and cybersecurity tools within its cloud offering. Allegations from competitors such as Google Cloud and Nextcloud underscore the concern that Microsoft uses its dominance in core software markets to steer customers toward its cloud services.

In 2022, the Dutch Authority for Consumers and Markets (ACM) published a market study into cloud services, highlighting how smaller providers struggle to compete with large, integrated players.[37] The study also assessed whether competition in cloud services is operating effectively and examined potential risks to pricing, quality, and innovation arising from market structures, commercial practices, and technical configurations. This imbalance is reinforced by vendor lock-in, weak interoperability, and switching barriers. Although the ACM initiated a follow-up investigation into these competition concerns, it ultimately decided to pause further action, citing confidence that the Data Act and the DMA would address several of the key issues. Nonetheless, the ACM has made clear that it remains ready to reopen the case if new evidence emerges.

---

35 European Commission. Commission carries out unannounced antitrust inspections in the data centre construction sector. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5926

36 CISPE (2024). CISPE and Microsoft Agree Settlement in Fair Software Licensing Case. Available at https://cispe.cloud/cispe-and-microsoft-agree-settlement-in-fair-software-licensing-case/. CISPE (2025). European Cloud Observatory (ECO). Available at https://cispe.cloud/ecco.

37 ACM. (2022). Market study into cloud services. Available at: https://www.acm.nl/en/publications/market-study-cloud-services.

Similarly, the French Autorité de la Concurrence launched an investigation into the cloud market, focusing on the dominance of AWS, Google, and Microsoft Azure.[38] The inquiry examined not only cloud infrastructure but also data centre operations and broader service offerings. The Autorité raised concerns that the entrenched positions of these major providers may hinder market entry and growth for smaller players. It suggested that the European Commission could leverage the DMA to address key issues such as egress fees, the use of cloud credits, and the lack of interoperability and portability. The French authority also signalled its intention to actively pursue enforcement using its national competition powers. These inquiries form part of the Commission's broader agenda to scrutinise structural barriers and unfair business practices in digital infrastructure markets.[39]

These and other cases (for an overview, see Table 2) illustrate how tying identity, security, and AI functions into essential productivity or cloud suites can impede switching and cloud customer choice, risking exclusion of rivals in adjacent software, AI application, and cybersecurity markets.

TABLE 2: INVESTIGATIONS AND COMPLAINTS OPENED AGAINST CLOUD SERVICES AND AI COMPANIES

Country	Cloud Service Provider – AI company	Purpose	Source
EU	Microsoft (2020)	In 2020, Slack Technologies filed a formal complaint with the European Commission, alleging that Microsoft had illegally tied its Teams application to its dominant Office 365 and Microsoft 365 productivity suites – a move that triggered the Commission's current antitrust investigation into possible abuse of market dominance under EU competition law. In April 2024, Microsoft announced it would stop bundling its Teams videoconferencing app with Office globally.	European Commission (2020), Antitrust: Commission opens investigation into possible anticompetitive practices by Microsoft regarding Teams. Available at https://ec.europa.eu/commission/presscorner/detail/hu/ip_23_3991. Also see Fortune (2024), Microsoft stops bundling Teams with Office after a complaint from Slack triggered antitrust scrutiny. Available at https://fortune.com/europe/2024/04/01/microsoft-splits-teams-office-eu-antitirust-probe-slack-bundling-complaint/.
UK	Microsoft and OpenAI (2023)	An initial information gathering step in advance of the launch of any formal investigation—into the partnership between Microsoft and OpenAI	Press Release, CMA, CMA seeks views on Microsoft's partnership with OpenAI (Dec. 8, 2023), https://www.gov.uk/government/news/cma-seeks-views-on-microsofts-partnership-with-openai
UK[40]	Microsoft and Inflection AI (2024)	Launched a merger inquiry regarding Microsoft's transaction with Inflection AI in July 2024	Microsoft / Inflection inquiry, CMA (Apr. 24, 2024), https://www.gov.uk/cma-cases/microsoft-slash-inflection-aiinquiry

[38] Autorite de la Concurrence. (2023). Cloud computing: the Autorité de la concurrence issues its market study on competition in the cloud sector. Available at: https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud

[39] European Commission. (2024). Commission carries out unannounced antitrust inspections in the data centre construction sector. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_5926/IP_24_5926_EN.pdf

[40] The CMA has since closed these investigations.

Country	Cloud Service Provider – AI company	Purpose	Source
UK	Amazon and Anthropic (2024)	Launched an investigation of Amazon's partnership with Anthropic	Amazon / Anthropic partnership merger inquiry, CMA (Apr. 24, 2024), https://www.gov.uk/cma-cases/amazon-slash-anthropic-partnership-merger-inquiry
UK	Google and Anthropic (2024)	Launched an investigation into the Google-Anthropic partnership	Alphabet Inc. (Google LLC) / Anthropic merger inquiry, CMA (July 30, 2024), https://www.gov.uk/cma-cases/alphabet-inc-google-llc-slash-anthropic-merger-inquiry
EU	Microsoft (2022)	European Commission investigated a competition complaint filed by CISPE.	CISPE (2024). CISPE and Microsoft Agree Settlement in Fair Software Licensing Case, https://cispe.cloud/cispe-and-microsoft-agree-settlement-in-fair-software-licensing-case/. CISPE (2025). European Cloud Observatory (ECO), https://cispe.cloud/ecco.
EU	Microsoft and OpenAI (2024)	Investigation in the agreements between "large digital market players and generative AI developers and providers" and specifically whether "Microsoft's investment in OpenAI might be re-viewable under EU Merger Regulation."	Press Release, European Commission, Commission launches calls for contributions on competition in virtual worlds and generative AI (Jan. 8, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_85/ https://www.theguardian.com/technology/2024/jan/09/microsoft-investment-openai-chatgpt-european-union-eu-merger-investigation
EU	Microsoft (2023)	OVHcloud, Aruba, and the Danish Cloud Community – filed a complaint with the Commission alleging that Microsoft abused its dominance in productivity software (e.g. Office 365) to favour its own Azure cloud infrastructure. The complaint centred on licensing terms that penalised customers for running Microsoft software on third-party infrastructure.	The Register (2025). Euro cloud providers react to MS potentially cutting deal on antitrust. Available at https://www.theregister.com/2023/03/30/microsoft_euro_complaints/
France	Microsoft, OpenAI, Amazon, Google, Anthropic (2024)	Opened inquiries ex officio to analyse the generative AI market and "examine these types of investments" such as Microsoft's investment into OpenAI and Amazon and Google's investments into Anthropic[41]	Press Release, Autorité de la Concurrence, Generative artificial intelligence: the Autorité starts inquiries ex officio and launches a public consultation open until Friday, 22 March (Feb. 8, 2024), https://www.autoritedelaconcurrence.fr/en/press-release/generative-artificial-intelligence-autorite-starts-inquiries-ex-officio-and-launches

[41] While competitive concerns in cloud computing persist, it is important to also consider the impact of generative AI, which is reshaping the cloud market. New GenAI platform services, GPU-as-a-service offerings, and enhancements across cloud services are driving growth. In terms of market positioning, Amazon continues to lead with a 30% share, though Microsoft (21%) and Google (12%) recorded faster growth rates in Q4. Among second-tier providers, CoreWeave, Oracle, Snowflake, Cloudflare, and Databricks saw the highest year-on-year growth, with CoreWeave notably entering the top twenty cloud providers due to its AI and GPU services. If we narrow our focus to specific layers of cloud computing, particularly those boosted by AI integrations, the sector does show strong signs of competition. See: Synergy Research Group. (2025). Cloud Market Jumped to $330 billion in 2024 – GenAI is Now Driving Half of the Growth. Available at: https://www.srgresearch.com/articles/cloud-market-jumped-to-330-billion-in-2024-genai-is-now-driving-half-of-the-growth.

Country	Cloud Service Provider – AI company	Purpose	Source
France	SAP (2021)	Filed a complaint accusing the firm of unfair bundling and pricing practices in its ERP software market.	Cigref (2022), Le Cigref saisit l'Autorité de la concurrence pour pratiques anticon-currentielles de cer-tains éditeurs de lo-giciels. Available at https://www.cigref.fr/le-cigref-saisit-lautorite-de-laconcur-rence-pour-pratiques-anticoncurrenti-elles-de-certains-editeurs-de-logiciels
Germany	Microsoft (2023/2024)	Germany's competition authority has designated Microsoft as a company of "paramount cross-market signifi-cance", granting it powers to act against anti-competitive behaviour not cov-ered by the EU's Digital Markets Act – particularly in cloud and AI services. The Bundeskartellamt aims to close regulatory gaps, citing Microsoft's tightly integrated ecosystem and dominance in key software markets. Ongoing complaints from rivals like Google and Nextcloud allege unfair licensing prac-tices that pressure customers to choose Microsoft's cloud over others. While Microsoft has settled some cases, reg-ulators in Germany, the UK, and beyond are stepping up scrutiny.	The Register (2024), Germany is mon-itoring Microsoft to thwart 'anti-com-petitive practices'. Available at https://www.theregister.com/2024/10/01/german_regulators_monitor_micro-soft/. Also see Bundeskartellamt (2024), Microsoft also subject to extended abuse control pursuant to Section 19a GWB – Bundeskartellamt determines paramount significance across markets. Available at https://www.bundeskar-tellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/30_09_2024_Microsoft_19a.html.

Source: ECIPE compilation.

4.2 Lessons from the UK Cloud Services Market Investigation

The UK Competition and Markets Authority (CMA) provisionally concluded in January 2025 that several features of the cloud services market in the UK restrict competition, particularly due to technical and commercial barriers to switching and multi-cloud use, and software licensing practices.[42] The CMA identified "adverse effects on competition" stemming from bundling, licensing constraints, egress fees, and hyperscaler business practices. It proposed that future enforcement should rely on new digital markets powers, including the potential designation of AWS and Microsoft with Strategic Market Status (SMS).[43] In doing so, the CMA initiated a far-reaching discussion about the structure and functioning of the UK cloud market.

[42] While other national authorities, including in the Netherlands and France, have also investigated similar concerns, the UK CMA's cloud market investigation is currently the most comprehensive and advanced in procedural terms. Its provisional remedies and proposed use of new digital markets powers offer concrete insights into potential regulatory approaches, which is why the CMA's findings are highlighted here. We nonetheless acknowledge that future drafts may benefit from integrating key parallels or contrasts from other national reports. See UK Competition and Market Authority (CMA). Cloud services market investigation – The Competition and Markets Authority (CMA) is investigating the supply of public cloud infrastructure services in the UK. Available at https://www.gov.uk/cma-cases/cloud-services-market-investigation.

[43] UK Competition and Market Authority (CMA). Cloud Services Market Investigation. Summary of provisional decision, 28 January 2025. Available at https://assets.publishing.service.gov.uk/media/67989251419bdbc8514fdee4/summary_of_provisional_decision.pdf.

The provisional remedies focused on reducing customer lock-in and restoring competitive neutrality, particularly in relation to the largest providers. While many stakeholders, especially challenger firms, SMEs, and civil society organisations broadly welcomed the CMA's findings and recommended going further in certain areas, others expressed caution.

Several respondents, including Microsoft, AWS, and affiliated industry associations, argue that the CMA overstates the risks of foreclosure and underestimates the benefits of integration, scale, and pricing flexibility. Some warned that broad intervention could stifle innovation or raise costs for end-users. As a result, the debate on cloud competition in the UK has become both a technical and political challenge, involving trade-offs between interoperability, commercial freedom, and user protection.

While the CMA's provisional findings and remedies focus primarily on AWS and Microsoft, this does not imply that concerns around customer lock-in, interoperability, and licensing are limited to these providers. Similar practices and structural features can be observed across parts of the wider cloud services market, including among other major and regional providers. The analysis here should therefore be understood in a broader, provider-neutral context.

The following sections outline the sixteen most recent stakeholder responses to the CMA's provisional findings and highlight market concerns across four key features: bundling, licensing, cloud credits, and egress fees.[44] While these findings stem from the UK market investigation, they are directly relevant for the EU, where similar concerns have been raised in policy debates and regulatory consultations. Given the global nature of cloud markets and the cross-border operations of leading providers, the CMA's analysis offers important insights for EU policymakers seeking to strengthen competition, ensure interoperability, and reduce switching barriers in line with the goals of the Data Act and broader digital strategy.

[44] As of June 23, 2025. See https://www.gov.uk/cma-cases/cloud-services-market-investigation.

4.2.1 Bundling

The CMA's investigation raised concerns that bundling of software with cloud infrastructure may distort competition by locking customers into ecosystems and limiting the viability of alternative providers. Several stakeholders particularly from challenger firms and cloud competitors supported this concern, citing exclusionary effects in public sector procurement and enterprise environments. However, some large providers and affiliated commentators argued that bundling is a standard commercial strategy that reflects legitimate demand for integrated solutions, not necessarily an attempt to foreclose rivals.

TABLE 3: RESPONSES TO CMA PROVISIONAL FINDINGS, STAKEHOLDER VIEWS ON BUNDLING PRACTICES

Stakeholder	Summary of Position
AWS	Defends bundling as customer-driven integration, enabling innovation.
Blackbox Hosting	No specific comment.
CCIA	Bundling is standard and not inherently anti-competitive.
Civo	No comment.
Cloudflare	Bundling harms competition; favours dominant firms.
Dr Baker, Oxford Cross Disciplinary Machine Learning Research Cluster (OXML)[45]	Claims bundling concerns lack empirical foundation.
Google	Bundling by Microsoft is exclusionary (e.g., Dynamics365).
ICLE	Warns against overreach; bundling delivers value.
Microsoft	Customers benefit from integrated services; bundling is voluntary.
Open Cloud Coalition	Bundling distorts access to AI and enterprise tools.
OVHcloud	Bundling entrenches dominance, esp. in AI services.
Prolinx	Exclusion of SMEs in defence sector due to bundling.
Rayo	Customers value bundled offers.
Rob Sedgwick	No view.
Simon Hansford	Bundling locks in public sector cloud contracts.
Startup Coalition	Neutral; notes bundled offers may benefit startups.

Source: ECIPE compilation.

[45] As stated in the consultation note, Microsoft provides support for the Cross-Disciplinary Machine Learning Research Cluster at Wolfson College, University of Oxford (OXML).

4.2.2 Licensing

The CMA provisionally found Microsoft's licensing practices to be a significant restriction on competition in the cloud market, particularly through discriminatory pricing and technical barriers that make it harder to use Microsoft software on non-Microsoft cloud infrastructure. This view was widely supported among challengers and rival cloud service providers, who described such licensing as a major obstacle to multi-cloud adoption. However, Microsoft and some industry bodies argued that the CMA mischaracterised licensing norms and ignored the commercial logic underpinning enterprise software models.

TABLE 4: RESPONSES TO CMA PROVISIONAL FINDINGS, STAKEHOLDER VIEWS ON LICENSING PRACTICES

Stakeholder	Summary of Position
AWS	Critiques Microsoft's discriminatory licensing; promotes its own transparent terms.
Blackbox Hosting	No direct comment.
CCIA	Opposes CMA intervention; sees no abuse.
Civo	No view.
Cloudflare	No comment.
Dr Baker, Oxford Cross Disciplinary Machine Learning Research Cluster (OXML)	Criticises CMA's economic rationale; defends licensing norms.
Google	Highlights Microsoft's pricing and usage restrictions on rivals.
ICLE	Licensing concerns overstated; competition still viable.
Microsoft	Strongly defends its software terms as commercially fair.
Open Cloud Coalition	Supports CMA; sees licensing as a tool of market capture.
OVHcloud	Licensing distorts cloud economics; backs remedies.
Prolinx	UK sovereignty requires open licensing.
Rayo	No view.
Rob Sedgwick	Shares negative personal licensing experience.
Simon Hansford	Calls Microsoft's practices "predatory" and anticompetitive.
Startup Coalition	Supports interoperable licensing; cautious on heavy intervention.

Source: ECIPE compilation.

4.2.3 Cloud Credits

Cloud credits often offered in large sums by large technology companies to start-ups, AI firms, or public institutions were not the focus of specific CMA remedies but nonetheless emerged as a major issue in stakeholder feedback. Several providers argued that these credits act as a powerful early-stage lock-in mechanism, deterring customers from exploring alternative services. Others, particularly large technology companies and start-up advocates, view them as a pro-competitive tool that reduces upfront costs and fosters innovation. This disagreement highlights the tension between incentives that appear benign at the customer level but may entrench market power at scale.

TABLE 5: RESPONSES TO CMA PROVISIONAL FINDINGS, STAKEHOLDER VIEWS ON CLOUD CREDITS

Stakeholder	Summary of Position
AWS	Silent, implies they're legitimate incentives.
Blackbox Hosting	Credits distort SME competition; tied to VC networks.
CCIA	No position.
Civo	Calls credits "Trojan horses" for vendor lock-in.
Cloudflare	No view.
Dr Baker, Oxford Cross Disciplinary Machine Learning Research Cluster (OXML)	No position.
Google	Silent, presumed supportive.
ICLE	Defends as normal commercial practice.
Microsoft	Justifies as standard cost-offset tools.
Open Cloud Coalition	Criticises effect on SME and public procurement.
OVHcloud	Calls credits a long-term lock-in strategy.
Prolinx	Credits tilt the playing field against small providers.
Rayo	No comment.
Rob Sedgwick	No comment.
Simon Hansford	Credits dominate early-stage and AI provider selection.
Startup Coalition	Supports credits; essential for startup viability.

Source: ECIPE compilation.

4.2.4 Egress Fees

Data egress fees, the costs of moving data out of a cloud provider's environment, were identified by the CMA as a material barrier to switching and multi-cloud use. Most challengers agreed and called for removal or zero-rating of such fees, particularly for public sector or regulated workloads. In contrast, major providers argued that egress fees reflect fair usage costs and removing them could lead to higher prices elsewhere. The responses underscore a broader debate about whether switching costs are an outcome of customer inertia or a result of deliberate architectural and pricing strategies.

TABLE 6: RESPONSES TO CMA PROVISIONAL FINDINGS, STAKEHOLDER VIEWS ON EGRESS FEES

Stakeholder	Summary of Position
AWS	Opposes regulation; warns of unintended price effects.
Blackbox Hosting	Supports intervention; fees are a switching barrier.
CCIA	Silent.
Civo	Wants fees abolished; calls them technical and financial obstacles.
Cloudflare	Supports CMA; fees reduce market dynamism.
Dr Baker, Oxford Cross Disciplinary Machine Learning Research Cluster (OXML)	Minimises impact; calls fees a pricing choice.
Google	Cautious; warns against one-size-fits-all approach.
ICLE	Sceptical of impact; warns against blunt remedies.
Microsoft	Argues switching is possible; defends fees as fair cost allocation.
Open Cloud Coalition	Calls for zero-rated egress for public sector users.
OVHcloud	Advocates total fee removal to foster switching.
Prolinx	Supports removal to aid UK digital autonomy.
Rayo	Downplays importance; says affects few clients.
Rob Sedgwick	Calls for CMA to go further.
Simon Hansford	Supports removal; part of broader market distortion.
Startup Coalition	Neutral; few startups affected but caution against cost shifts.

Source: ECIPE compilation.

4.3 Bundling and Licensing in the Age of AI

The vertical integration of large technology companies from IaaS, through platforms (PaaS), to applications (SaaS) now extends to foundational AI capabilities such as large language models, vector databases, and GPU-as-a-service offerings. These integrated stacks offer unprecedented benefits in terms of innovation, speed, and ease of use but also raise pressing concerns about lock-in and long-term market concentration.

Leading cloud providers can now embed proprietary AI models directly into productivity software, video call apps, developer tools, and data platforms. Microsoft's Copilot suite and Google's Gemini integrations exemplify this dynamic: customers are offered AI-enhanced tools as seamless extensions of familiar applications. This bundling accelerates AI adoption across individual users, SMEs, and public institutions. By lowering the cost and complexity of accessing advanced models, these firms are playing a key role in technology diffusion helping mainstream institutions take advantage of powerful capabilities without in-house expertise.

Yet the same bundling strategies that enable rapid innovation and deployment can also entrench market power, particularly when integration extends beyond AI tools to core enterprise functions such as identity management and cybersecurity. Bundling these critical features into broader software or infrastructure packages can deepen vendor lock-in and raise serious competition concerns. Regulators in both Europe and the U.S. have flagged this practice. The European Commission's ongoing probe into Microsoft's Entra ID (formerly Azure AD) is examining whether licensing terms restrict customers from choosing rival identity providers such as Okta or Cloudflare.[46] The Commission's earlier action against Microsoft's bundling of Teams with Office 365 underscores broader apprehension about how tying dominant software to ancillary services can create structural dependencies.[47] In parallel, the U.S. Federal Trade Commission (FTC) is examining whether Microsoft's bundling of advanced cybersecurity tools – particularly when offered in government contracts has the effect of locking in customers by erecting switching barriers.[48]

As major technology firms like Google, Amazon, and Microsoft expand their control across the AI value chain from proprietary chips (e.g. Google TPUs, AWS Trainium) to cloud infrastructure, model APIs, and developer platforms they are effectively consolidating the entire "vertical AI stack". By owning each layer, these firms can optimise performance within their ecosystem while making interoperability with other providers more difficult, reinforcing customer lock-in and reducing opportunities for open-source or specialist models to compete.

Several regulators have acknowledged the structural risks. The European Commission and the U.S. FTC are investigating whether bundling of AI tools with cloud services or software suites raises

[46] BIS (2024). What EU Antitrust Probe Around Entra ID Means for Microsoft. Available at https://www.bankinfosecurity.com/blogs/what-eu-antitrust-probe-around-entra-id-means-for-microsoft-p-3570?utm_source=chatgpt.com.

[47] Computer Weekly (2024). European Commission declares Microsoft's bundling of Teams with M365 anti-competitive. Available at https://www.computerweekly.com/news/366589856/European-Commission-declares-Microsofts-bundling-of-Teams-with-M365-anti-competitive?utm_source=chatgpt.com.

[48] Bloomberg (2024). Microsoft Faces Broad Antitrust Investigation From US FTC. Available at https://www.bloomberg.com/news/articles/2024-11-27/us-antitrust-watchdog-launches-broad-microsoft-investigation?utm_source=website&utm_medium=share&utm_campaign=copy&embedded-checkout=true.

foreclosure risks, particularly when tied to long-term licensing contracts, volume-based rebates, or restrictive terms on interoperability. The European Commission is examining whether exclusive partnerships, such as Microsoft's with OpenAI, hinder competition in cloud-based AI services.[49] Similarly, the U.S. FTC has launched antitrust probes into cloud–AI partnerships and licensing practices that may create structural dependencies.[50] The UK CMA's investigation into cloud services – published in its 28 January 2025 provisional decision – recognises the transformative impact of AI but concludes that AI has not yet materially changed the core competition issues in cloud infrastructure.[51]

TABLE 7 MAJOR REGULATORY CONCERNS ABOUT BUNDLING IN THE AGE OF AI

Regulatory Body	Main Concerns	Key Examples	Policy Direction
UK CMA (2025)	Bundling of AI with cloud services may lock in users and undermine multi-cloud strategies; licensing and pricing practices reinforce these effects.	Microsoft Copilot on Azure; AWS AI stack	Encourages multi-cloud, portability, and scrutiny under SMS rules
European Commission (2024)	Vertical integration risks entrenching dominant platforms across the AI stack; exclusive access to foundation models may restrict rivals.	Microsoft–OpenAI partnership; Google–Gemini integration	Examining potential harm to competition and future regulatory tools
U.S. FTC (2024)	AI partnerships and bundling may distort the market by concentrating compute, data, and model access in a few hands.	Microsoft–OpenAI, Amazon–Anthropic, Google–Anthropic	Conducting 6(b) inquiry into partnerships; outcomes may inform future enforcement

Source: ECIPE compilation.

The growing concentration of infrastructure, model access, and developer tooling may result in a less contestable AI ecosystem, one where customers face high switching costs and where market entry for new providers becomes increasingly difficult. Similar risks have already materialised in the cybersecurity domain, where bundling of identity and security services into dominant productivity suites has limited interoperability and reinforced customer dependence. These dynamics can extend into AI: vendors are often required to deploy their services directly on a large cloud platform to access cloud marketplaces, while committed spend deals and large cloud credits further bind customers to tightly integrated ecosystems. These credits, which often

[49] European Commission (2024). Competition Policy Brief – Competition in Generative AI and Virtual Worlds. Available at https://competition-policy.ec.europa.eu/document/download/c86d461f-062e-4dde-a662-15228d6ca385_en.

[50] U.S. FTC (2024). FTC Launches Inquiry into Generative AI Investments and Partnerships – Agency Issues 6(b) Orders to Alphabet, Inc., Amazon.com, Inc., Anthropic PBC, Microsoft Corp., and OpenAI, Inc. Available at https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships. Also see U.S. FTC (2023). Generative AI Raises Competition Concerns. Available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns?.

[51] UK Competition and Markets Authority (CMA, 2025). Cloud Infrastructure Services – Provisional decision report, 28 January 2025. Available at https://assets.publishing.service.gov.uk/media/6798ecb1419bdbc8514fdf8a/cloud_mi_provisional_decision_report.pdf. As concerns the partnership between Microsoft and OpenAI , the UK Competition and Markets Authority (CMA) reviewed Microsoft's partnership with OpenAI and concluded in March 2025 that it does not qualify as a relevant merger situation under UK merger control rules. While the CMA recognises that Microsoft's role as cloud provider and key partner to OpenAI is commercially significant, it ultimately concluded that the partnership does not give Microsoft control over OpenAI and thus does not trigger merger review powers. However, this does not preclude scrutiny under other regulatory tools, such as Strategic Market Status (SMS) designation under the UK's Digital Markets, Competition and Consumers (DMCC) regime. See UK Competition and Markets Authority (CMA, 2025). Microsoft Corporation's partnership with OpenAI, Inc., Decision on relevant merger situation. Available at https://assets.publishing.service.gov.uk/media/67fe26ef712bf73dea135449/____Full_text_decision__.pdf.

enable innovation adoption, can also function as early-stage lock-in mechanisms especially when offered conditionally on usage quotas, service bundling, or proprietary tool adoption.[52]

Vertical reach enables providers to shape not just competition within each layer, but also the terms of access across the stack. For example, a cloud provider may sell basic infrastructure to third parties while also offering its own competing applications creating an incentive to favour its own software through bundling, pricing, or technical compatibility. Amazon's entry from infrastructure to platform and now application services, including AI tools, illustrates this shift, as does Microsoft's integration of its AI models across Azure and productivity applications. [53]

The convergence of cloud and AI capabilities makes it important for competition authorities to scrutinise bundling and licensing practices. While feedback loops and network effects may be weaker in AI than in traditional platforms, within-user learning (e.g. personalisation) still creates compounding switching costs.

At the same time, the policy response should not be blunt. Bundling and standardisation need not be at odds. AI tools can and should be embedded in cloud offerings but also made interoperable. Many enterprises are pursuing multi-cloud or hybrid strategies to mitigate dependency, optimise performance, and diversify risk. The growth of containerised workloads, open-source orchestration tools like Kubernetes, and cloud-agnostic machine learning frameworks is reducing technical barriers to switching. What is needed is a market environment that supports those choices through regulatory clarity and technical compatibility.

Supporting voluntary interoperability standards particularly around model portability, inference workloads, and access to foundational models across providers is essential. Regulators should champion cloud neutrality, not by banning bundling outright, but by ensuring customers can choose, combine, and exit cloud services without disproportionate penalty. This is especially important in public sector adoption of AI, where procurement decisions today may shape vendor dependency for decades to come. A contestable cloud-based AI ecosystem will depend not just on innovation, but on the governance of the infrastructures through which innovation is delivered.

It is equally important to recognise that proprietary AI tools have been instrumental in broadening access to cutting-edge technologies. As the European Commission's AI enforcement briefings note,[54] large technology companies have rapidly scaled state-of-the-art models and embedded them into consumer, business, and public sector tools accelerating AI diffusion across Europe. Services like Microsoft's Copilot or Google's Gemini enable millions to benefit from advanced AI capabilities without needing in-house expertise or infrastructure. This demonstrates the productivity and innovation potential of platform-led integration. The Commission's briefing note

---

[52] UK Competition and Markets Authority (CMA, 2025). Cloud services market investigation – Responses to provisional findings, submission by Cloudflare. Available at https://assets.publishing.service.gov.uk/media/67c188c8a0f0c95a498d20ea/Cloudflare_response_to_provisional_decision.pdf.

[53] Jenny, F. (2023). Unfair Software Licensing Practices: A quantification of the cost for cloud customers. Available at: https://cispe.cloud/website_cispe/wp-content/uploads/2023/06/Quantification-of-Cost-of-Unfair-Software-Licensing_Prof-Jenny_-June-2023_web.pdf

[54] European Commission (2024). Competition Policy Brief – Competition in Generative AI and Virtual Worlds. Available at https://competition-policy.ec.europa.eu/document/download/c86d461f-062e-4dde-a662-15228d6ca385_en.

recognises that large digital firms have contributed to the diffusion of generative AI by enabling smaller developers to access critical infrastructure, capital, and distribution channels, fostering innovation and broader market participation, while also noting the need for competition oversight (see Table 8).

TABLE 8: POSITIVE CONTRIBUTIONS BY LARGE FIRMS IN THE COMMISSION BRIEFING NOTE

Area	Description from Briefing Note	Commission Assessment
Infrastructure Access	Large firms provide cloud capacity and compute power through partnerships with smaller AI developers	Can be pro-competitive when access is non-exclusive
Capital and Resources	Investments by large players help smaller firms develop and scale AI models	Viewed as important for technological progress
Distribution Channels	Integration of smaller models into established products increases reach	Considered efficient when it expands access for innovators
Complementary Capabilities	Partnerships combine financial, technical, and market knowledge	Recognised as a source of innovation and efficiency gains
Knowledge Diffusion	Collaborations disseminate expertise and accelerate development	Supports market-wide innovation
Model Diversity	Development of both open-source and proprietary models by large and mid-sized firms	Enhances innovation and lowers entry barriers

Source: ECIPE compilation.

As concerns competition over time (when we say competition, we mean dynamic competition), competition enforcement must not come at the cost of entrenching dominance. Effective competition enforcement should aim not only to prevent exclusionary practices but also to preserve the conditions for new entrants and decentralised innovation to flourish alongside the giants.[55]

A key question is whether customers are truly locked into a single cloud provider over time. Many businesses and (less so) public sector organisations already pursue multi-cloud or hybrid strategies to optimise cost, performance, and resilience. While lock-in and switching costs can be high, especially for complex legacy systems, they are not insurmountable. Newer applications built with cloud-agnostic tools such as Kubernetes, Linux-based environments, and open-source databases like PostgreSQL and MySQL – make migration and multi-homing increasingly feasible.

At the same time, generative AI is reshaping cloud market dynamics over time. New services such as GenAI platforms, GPU-as-a-service, and AI-enhanced infrastructure are driving growth and innovation. Amazon currently is the market leader with 30% share, but Microsoft (21%) and Google (12%) are gaining ground. Second-tier players like CoreWeave, Oracle, Snowflake,

[55] Blomstein (2024). Generative AI in the Antitrust Spotlight: EU Regulators Gear Up. Available at https://www.blomstein.com/assets/downloads/240216_briefing_ai-briefing-series_eu-competition-regulation.pdf. Also see EESC (2025). Generative AI and foundation models in the EU: Uptake, opportunities, challenges, and a way forward. Available at https://www.eesc.europa.eu/sites/default/files/2025-03/QE-01-25-014-EN-N_0.pdf.

Cloudflare, and Databricks are expanding rapidly, suggesting that competition is intensifying, particularly in AI-driven service layers.[56]

IT decision-makers often cite cost-related factors such as the loss of software discounts or challenges with licence portability rather than outright exclusion as reasons for remaining with incumbent providers. Familiarity with specific ecosystems, bundled service offerings, and long-standing supplier relationships also shape customer choices. These factors can entrench dominant providers, yet they often reflect rational trade-offs rather than deliberate anti-competitive conduct.

The same logic applies to cybersecurity: integrated security features – whether offered as part of a single cloud provider's suite, a bundled third-party package, or via an external specialist with access to cloud data traffic can enhance operational efficiency and reduce response times by consolidating protection layers. These configurations often offer convenience, stronger baseline protection, and simplified accountability, particularly in sensitive domains such as defence or public sector AI use, where ministries may favour integrated setups to reduce the number of external interfaces and enhance control.

However, recent high-profile incidents, such as the CrowdStrike failure in 2024, have highlighted a key vulnerability of integrated models: they may introduce single points of failure that can cascade across systems when critical services are tightly coupled. This has amplified calls for greater modularity and redundancy, with some security experts advocating for the separation of critical functions and more flexible deployment models that allow substitution without compromising compatibility.

Ultimately, while integrated offerings may reinforce customer reliance on a specific vendor – especially when optimised for proprietary environments – they are not inherently anti-competitive. What matters is the freedom to choose, the ease of substitution, and the ability to tailor security configurations to risk profiles and regulatory needs. EU policy should therefore focus on enabling transparent, interoperable, and accountable security architectures, rather than prescribing a one-size-fits-all model.

Moreover, several mitigating forces counterbalance these risks. Open-source environments, containerisation, and microservices reduce technical dependency, while voluntary standards and data portability initiatives lower migration barriers. Competition policy should focus on clear cases of exclusion and market distortion, not penalise efficiency or legitimate loyalty incentives. Promoting open standards and interoperability is key to keeping the cloud ecosystem contestable. It is therefore essential that regulatory enforcement distinguishes between pro-competitive integration and exclusionary conduct. Misguided intervention risks penalising efficiency and innovation and ignoring major technology providers' sometimes subtle tactics to thwart competition.

[56] Synergy Research Group. (2025). Cloud Market Jumped to $330 billion in 2024 – GenAI is Now Driving Half of the Growth. Available at: https://www.srgresearch.com/articles/cloud-market-jumped-to-330-billion-in-2024-genai-is-now-driving-half-of-the-growth

Rather than rigid constraints, regulators should encourage industry-led standardisation as a more effective way to protect cloud customer choice. As the market becomes more fragmented and new players grow in specialised niches, lessons from the global cellular sector show that interoperability can support competition without dismantling integration benefits. This approach is explored in the next section.

5. STANDARDISATION IN LIGHT OF GROWING CLOUD MARKET SPECIALISATION

The cloud sector's growing complexity, coupled with competition challenges and the increasing specialisation of providers, could also be addressed in ways that are different from the existing regulatory track and from antitrust enforcement. A more efficient framework for cloud service standards and policy guidance on a market architecture based on FRAND principles is a complementary approach with significantly huge payoffs for the entire market, allowing for more specialisation and interoperability across services and user demands.

Standardisation is not a silver bullet and developments so far for cloud service standards have been slow. However, a system based on direct policy guidance on FRAND principles for markets and contracts would be fundamentally different from the current standards framework for cloud, especially if it is also pioneered in public procurement. A market that moves in the direction of basic service standards and rules on licenses and interoperability would allow for more competition and specialisation without having rigid regulations. In other and adjacent sectors, such an approach has also proven useful for competition enforcement and to avoid having big court battles on contracts and technology products.

Moreover, it allows smaller providers to interoperate with widely used cloud technology ecosystems and empowers users to design cloud architectures aligned with their needs. Common technical standards could help promote customer migration, lower barriers to entry, and open up access to new markets by establishing clear, predictable rules for all market participants. A strategic, industry-led approach to cloud standardisation guided but not dominated by regulation would likely be the best tool for achieving more cloud customer choice. Introduction of standards can have pro-competitive effects.

However, the introduction of standards can also have unintended consequences if applied too rigidly or too early. When imposed on differentiated, innovation-driven products, premature standardisation may stifle technological development, limit market diversity, and ultimately weaken competition.

5.1 Lock-in by Licence: What FRAND May Solve

A persistent barrier to cloud customer choice stems from restrictive and discriminatory software licensing and contract practices. These practices, as outlined extensively above, are already observed by competition authorities, especially with the integration of AI tools into cloud and application ecosystems. Vendors may limit "Bring Your Own Licence" (BYOL) options or impose

surcharges when customers choose to run licensed software on third-party infrastructure, creating technical and financial lock-in. This reduces flexibility for multi-cloud or hybrid strategies, inflates switching costs, and raises rivals' costs – especially for smaller cloud providers trying to compete.

The principal issue is not new. In fact, it has been at the centre of several technology markets in the past that have featured technology acceleration, specialisation, and the legacy of competition dominated by large firms. For instance, the telecommunications sector faced similar challenges in the 1990s and early 2000s, particularly in the context of access to standard-essential technologies leading to "the smartphone war" and other conflicts between companies over licenses and access to markets. The resulting solution was to strengthen the bottom-up standard system and for the EU to develop fair, reasonable, and non-discriminatory (FRAND) licensing principles, designed to ensure access to patented technologies essential for industry-wide interoperability – such as in cellular networks. FRAND emerged through a combination of standard-setting organisation commitments, public policy guidance on framework rules for markets, and judicial clarification, including key rulings such as Huawei v ZTE by the European Court of Justice.[57] In that case, the Court balanced the patent holder's rights with obligations to offer non-discriminatory terms, ensuring that dominant players could not use access to essential technology as a tool for exclusion.

The EU Data Act, for instance, appears to take inspiration from this history. It identifies vendor lock-in as a barrier to competition and proposes technical interoperability through harmonised standards and open specifications (Recital 89) as the main remedy. However, this risks misdiagnosing the root cause of lock-in in today's cloud and AI markets. Many technical challenges in the cloud sector such as workload portability and API compatibility are already being addressed by market-led, open-source solutions, including Kubernetes and container orchestration tools. These tools enable cross-provider operability with increasing ease.

The deeper frictions lie in licensing and contract practices. Here, the Data Act attempts to repurpose FRAND originally developed for patents as a framework for governing data access and sharing. This design includes conceptual ambiguity and is not really solving problems. Unlike patents, data is not a fixed, formally registered asset. Its value is contextual and changes with timing, purpose, and platform capabilities. Cloud services and AI models evolve rapidly and are often proprietary in design, complicating the notion of what constitutes "fair and reasonable" access.

Furthermore, applying FRAND to many types of contractual terms between private parties with potential for third-party challenges based on perceived unfairness risks legal uncertainty. While courts have used FRAND as a tool to resolve disputes over access to essential technology, it is now being framed in the Data Act as a proactive compliance obligation, without established case law or institutional guardrails.

[57] WIPO (2015). Court of Justice of the European Union (Fifth Chamber) [2015]: Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH, Case No. C-170/13. Available at https://www.wipo.int/wipolex/en/text/591357. Also see Cleary Gottlieb (2015). Enforcing Standard-Essential Patents – The European Court of Justice's Judgment in Huawei v ZTE. Available at https://www.clearygottlieb.com/-/media/organize-archive/cgsh/files/publication-pdfs/enforcing-standard-essential-patents-the-european-court-of-justices-judgment-in-huawei-v-zte.pdf.

This conceptual ambiguity is also reflected in the European Commission's Final Report of the Expert Group on B2B Data Sharing and Cloud Computing Contracts (2025), which provides model contractual terms (MCTs) and standard clauses (SCCs) intended to support the implementation of the DA. While these templates are explicitly designed to reflect FRAND principles – particularly in cases where data access obligations apply – they stop short of defining what FRAND means in operational terms. Instead, the model clauses offer soft guidance on issues like reasonable compensation, liability, and contract termination, leaving room for flexible interpretation but also legal uncertainty. The report highlights that FRAND, originally crafted for essential patent licensing, and now serves more as a political and policy signal than a firm contractual benchmark – especially in fast-moving, service-based markets like cloud and AI.[58] This not only stretches the original scope of FRAND, but could also lead to increased litigation and regulatory overreach under the banner of fairness.

A better and more tailored approach would start with a standards framework with clearer rules for market participation and declared principles by participating firms what licensing and market rules that apply and not. This is not a structure to foreclose service provision by large companies but to make distinct on what services and on what conditions that interoperability applies. Specifically, helping to clarify and standardise portability rights and ensuring FRAND treatment across service and user domains, and through the full value chain, would:

- Promote transparency in procurement and licensing,
- Define operational practices for portability and interoperability (including when security or technical quality aspect should prevent interoperability),
- Clarify switching costs across cloud infrastructure providers,
- Support competition in adjacent service markets (e.g., productivity software, AI tools, databases), and
- Enable customers to select infrastructure based on performance and value – not on embedded licensing constraints.

To some, this may seem like an abstract concept but it is increasingly used in global technology markets, with clear and instructive examples already emerging in the cloud sector. In response to sustained regulatory and competitive pressure including formal complaints in the EU, Microsoft introduced a set of licensing reforms in 2022 under its European Cloud Principles.[59] These reforms aimed to address long-standing concerns raised by smaller and regional European cloud infrastructure providers.

- **Expanded Access to the Cloud Solution Provider (CSP) Programme:** Eligible European Cloud Providers (ECPs) typically regional and independent cloud operators are now permitted to participate in Microsoft's CSP programme. This

[58] European Commission (2025). Final Report of the Expert Group on B2B data sharing and cloud computing contracts. Available at https://www.aigl.blog/content/files/2025/04/Final-Report-of-the-Expert-Group-on-B2B-data-sharing-and-cloud-computing-contracts.pdf.

[59] Microsoft (2025). Microsoft announces new European digital commitments. Available at https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/; Microsoft (2023). European Cloud Principles: A year of progress. Available at https://blogs.microsoft.com/eupolicy/2023/05/17/european-cloud-principles-providers/; Microsoft (2022). Microsoft adopts European Cloud Principles. Available at https://blogs.microsoft.com/on-the-issues/2022/08/06/microsoft-adopts-european-cloud-principles/.

allows them to bundle Microsoft software such as Windows Server and SQL Server with their own infrastructure services and offer integrated billing and support. For example, OVHcloud in France can now offer Microsoft-licensed workloads bundled with its own infrastructure, delivering a seamless customer experience.

- **Introduction of the Flexible Virtualisation Benefit:** This benefit permits customers with eligible Microsoft subscriptions (e.g. with Software Assurance) to deploy their licences on cloud infrastructure run by Authorised Outsourcers, provided these are not designated as "Listed Providers" (i.e. AWS, Google Cloud, Alibaba). For example, a German SME with Microsoft 365 E3 licences can now deploy Office and Windows Server on PlusServer or T-Systems infrastructure without incurring additional BYOL penalties.

While Microsoft's 2022 reforms were a step toward addressing the competitive concerns of smaller European providers, the exclusion of major non-European cloud providers such as AWS, Google Cloud, and Alibaba from benefits like the Flexible Virtualisation programme undermines customer choice and access to third-part innovation.[60] There may be good reasons for such exclusion and there are reasons for many companies to observe caution in calling for unlimited interoperability – a free for all approach. However, a market framework that applies licensing flexibilities in a discriminatory manner risks undermining both innovation and overall market efficiency.

Looking ahead, the increasing vertical integration of AI into cloud platforms makes this issue even more urgent. Bundling foundation models or productivity tools with infrastructure services risks replicating old telecom lock-in problems at a new technological scale. Non-discriminatory licensing frameworks clearly defined, enforceable, and transparent would offer a more effective alternative to vague fairness doctrines or heavy-handed ex-ante regulation. They would protect competition without penalising innovation, and uphold platform neutrality while allowing integrated offerings to compete on merit.

5.2 A Path towards FRAND Licensing in Cloud Markets

To promote more interoperability, specialisation, and competition, EU lawmakers, competition authorities, and public procurement bodies could draw inspiration from the way FRAND licensing evolved in the cellular industry. This would involve combining industry-led initiatives with regulatory guidance and public sector incentives.

1. Defining What Should Be FRAND-Licensed

The first step is to identify which parts of the cloud and AI stack are essential for competition and should therefore be licensed on fair and non-discriminatory terms. These may include a "positive list" including for example:

[60] See, e.g., Microsoft (2024). Easily bring your licenses to the cloud. Available at https://www.microsoft.com/en-us/licensing/news/options-for-hosted-cloud.

- Critical APIs for interoperability, such as those enabling access to cloud infrastructure or foundation models;
- Software deeply integrated with infrastructure, like operating systems or productivity tools;
- Foundation models and AI platforms that become de facto standards due to widespread use.

Similarly, it should also be made clear what legitimate reasons can be used to limit access or the use of FRAND principles (a "negative list").

2. Encouraging Voluntary Industry Commitments

Just as holders of standard-essential patents (SEPs) have committed to FRAND licensing through bodies like ETSI or 3GPP, cloud and AI providers could adopt FRAND-like principles through voluntary participation in industry alliances and standards bodies.

The SEP experience also reveals the limits of regulatory enforcement. The European Commission's proposal for a SEP Regulation, which included a binding FRAND determination mechanism, faced significant opposition – particularly from licensees concerned about cost, legal complexity, and institutional overreach. The Commission ultimately withdrew the proposal in February 2025, citing a lack of stakeholder consensus.[61] This outcome underscores the challenges of top-down standard-setting and highlights the value of voluntary, market-led commitments in the cloud and AI context.

Relevant alliances include Gaia-X, the Linux Foundation, and the Open Compute Project, as well as international standards bodies (ISO, IEC, CEN, CENELEC). Commitments could focus on:

- Transparent, non-discriminatory access to APIs and interfaces;
- Equal licensing terms across deployment environments;
- Avoidance of technical lock-in.

Finally, the EU should resist developing EU-exclusive standards. Cloud and AI markets are global, and European competitiveness depends on international alignment, not regional fragmentation.

[61] European Commission (2025). European Commission Withdraws Proposals for Standard Essential Patents Regulation. Available at https://ec.europa.eu/newsroom/eismea/items/871191/en.

3. Clarifying Roles for Different Institutions

Several actors would need to work together to promote and enforce non-discriminatory licensing:

TABLE 9: FRAND LICENSING, ROLES FOR DIFFERENT INSTITUTIONS

Institution	Role
Standard-setting organisations (SDOs)	Should define key interfaces and require FRAND-style declarations from members, e.g., positive and negative lists, could issue voluntary Model Contractual Terms (MCTs) and Standard Contractual Clauses (SCCs)
European Commission (DG COMP)	Should issue guidance on licensing practices, guidance on positive and negative lists, issue voluntary Model Contractual Terms (MCTs) and Standard Contractual Clauses (SCCs),[62] update competition policy tools, and monitor compliance
National and EU courts	Should interpret and enforce FRAND obligations in specific cases, similar to the Huawei v ZTE ruling in telecoms
Public procurement agencies	Should require FRAND-compliant licensing for participation in public contracts and cloud services, based on work by SDOs as well as European Commission DG Comp
Cloud and AI vendors	Should adopt voluntary model clauses, publish transparent terms, and take part in licensing registries

Source: ECIPE compilation.

4. Promoting Transparency and Model Clauses

To avoid legal uncertainty, the EU and industry stakeholders could develop model clauses and guidelines for FRAND licensing in cloud and AI. This could include:

- Publicly accessible licensing registries
- Templates for standard terms and conditions
- Clear procedures for resolving licensing disputes

This would bring predictability and reduce the risk of litigation or regulatory overreach.

5. Using Public Procurement as a FRAND Catalyst

Governments and EU institutions could gradually use their purchasing power to encourage fairer licensing practices in cloud and AI markets. While there is currently no universal definition of non-discriminatory licensing in this context, public procurement policies can still promote broader principles of interoperability, openness, and competition. For instance, contracting authorities

[62] For example, to support the implementation of the EU Data Act, the European Commission's Expert Group on B2B Data Sharing and Cloud Computing Contracts has published a set of voluntary Model Contractual Terms (MCTs) and Standard Contractual Clauses (SCCs). These aim to simplify contract negotiations, reduce legal uncertainty, and foster trust in B2B data sharing and cloud services. The report discusses FRAND terms as a guiding principle in the drafting of both Model Contractual Terms (MCTs) and Standard Contractual Clauses (SCCs), particularly to implement Article 41 of the EU Data Act. See European Commission (2025). Final Report of the Expert Group on B2B data sharing and cloud computing contracts. Available at https://www.aigl.blog/content/files/2025/04/Final-Report-of-the-Expert-Group-on-B2B-data-sharing-and-cloud-computing-contracts.pdf.

could include objective, transparent criteria related to data portability, multi-cloud support, or published licensing terms – provided these are clearly linked to the contract's subject matter and compliant with EU procurement law.

Similarly, while the EUCS focuses on security assurance rather than licensing fairness, future iterations or complementary frameworks could consider incorporating elements of licensing transparency and lock-in mitigation. Importantly, the EUCS should remain non-discriminatory by default – ensuring that certification remains accessible to all providers that meet the required security criteria, regardless of their country of headquarters, business model, or licensing structure.

5.3 A Bottom-Up, Business-Led Agenda for Cloud Standardisation

Public regulation often plays an essential role in safeguarding competition and consumer rights, standards in markets for technology and digital services. However, when applied too rigidly or prematurely, top-down standardisation can inadvertently constrain innovation and entrench existing market structures. Mandating functional equivalence or imposing uniform service definitions across providers may suppress the very diversity that drives progress in the cloud sector.

A bottom-up approach would build on voluntary, industry-led standardisation efforts. These initiatives are often coordinated through open-source foundations, technical working groups, or sector-specific alliances. For instance, the Cloud Native Computing Foundation (CNCF) is a vendor-neutral, open-source foundation[63] that hosts and supports many of the most widely adopted technologies in cloud-native computing. Bottom-up standardisation models allow for greater adaptability, enabling providers to co-develop standards that accommodate the heterogeneity of services and customer needs. They also foster neutral governance, ensure faster innovation cycles, and encourage a dynamic and interoperable ecosystem without imposing rigid constraints. In highly innovative and diverse sectors such as cloud computing, these bottom-up processes offer a more effective and sustainable pathway to interoperability than top-down regulatory mandates.

Consider, Nerdalize, a Dutch company working with the CNCF,[64] deployed servers in residential heating systems to repurpose waste heat for hot water. This model reduced operating costs by up to 40% and cut household CO_2 emissions by around two tonnes per year. Each unit contained a server blade, cooled and redirected to heat domestic water. To orchestrate this distributed infrastructure, Nerdalize used Kubernetes, an open-source CNCF-hosted platform. This

[63] CNCF. Make Cloud Native Ubiquitous. Available at: https://www.cncf.io/.

[64] CNCF. Nerdalize: Providing affordable and sustainable cloud hosting with Kubernetes. Available at: https://www.cncf.io/case-studies/nerdalize/.

demonstrates how bottom-up standardisation, rather than centralised mandates, can support non-traditional, efficient, and interoperable deployments.[65]

Similarly, G Data's migration from Calico to Cilium both open, CNI-compliant Kubernetes networking tools illustrates how adherence to open standards improves agility. Faced with limited network visibility, G Data adopted Cilium (built on eBPF), enhancing observability, developer self-service, and security. This shift required no vendor lock-in or system overhaul. The case shows that open-standard platforms enable rapid adaptation, which is critical for innovation, security, and resilience in evolving cloud environments.[66]

A successful standardisation agenda for cloud computing must be led by business, grounded in real-world deployment needs, and responsive to commercial incentives. It should enable interoperability for key functionalities such as identity and access management, container orchestration, API design, and data portability while allowing diversity and innovation to thrive at the application level.

1. Industry Leadership on Core Cloud Technologies

Cloud standardisation must be driven by those who implement and operate the infrastructure – namely businesses and open-source developers, not primarily by academic institutions or consultative NGOs. Industry alliances and open-source communities such as CNCF, the Linux Foundation, and other vendor-neutral forums have delivered de facto standards like Kubernetes, Prometheus, and Cilium. These bodies succeed because they align technical development with market incentives and deployment timelines, something academic and civil society platforms often cannot do at speed or scale.

2. Inclusive – But Practically Oriented – Participation

While inclusiveness is important, standardisation must avoid becoming an academic exercise. SMEs, system integrators, enterprise users, and cloud-native startups must have a seat at the table – not just regulators or advocacy groups. European institutions should support underrepresented business voices in the process, especially those without dedicated policy teams, ensuring that standardisation reflects actual deployment challenges and commercial priorities.

3. Modular Design That Supports Adoption by Real Users

Cloud standards should target concrete, commercial interoperability pain points, not theoretical frameworks. Businesses require modular, incrementally adoptable standards that reflect the

[65] There are multiple layers involved in the standardisation efforts that supported Nerdalize's decentralised cloud model. At the orchestration layer, Kubernetes—an open-source, bottom-up developed platform—enabled workload management across distributed nodes. In networking, standard secure protocols such as VPNs, TCP/IP, and TLS encryption ensured safe and reliable connections between residential servers and the broader cloud infrastructure. At the hardware layer, standard x86 server components were adapted for custom cooling and heat reuse, building on existing modular server designs even though no formal regulatory standard applied. In system management, standard interfaces such as Prometheus monitoring and Kubernetes APIs allowed real-time infrastructure monitoring and interoperability across dispersed locations. Finally, at the physical integration layer, custom technical standards were developed to couple servers with household heating systems, generally following established HVAC and plumbing safety norms, even though no sector-wide formalisation existed.

[66] CNCF. G Data CyberDefense. Available at: https://www.cncf.io/case-studies/g-data-cyberdefense/

realities of hybrid and multi-cloud environments. Flexibility must remain a guiding principle – not academic purity.[67]

4. Fast-Track Industry-Led Approaches

Tools like CEN-CENELEC Workshop Agreements (CWAs) allow business stakeholders to rapidly create voluntary technical specifications that respond to urgent market needs. These fast-track processes are well suited to dynamic sectors like cloud computing and can be more effective than lengthy formal procedures disconnected from deployment cycles.

5. Early Consensus on Business-Critical Interfaces

As the mobile sector showed, standards on core interfaces (e.g. GSM, LTE) enabled global scale and investment. Similarly, early agreement on container runtimes, API specifications, and identity federation by cloud service providers and enterprise customers can unlock cross-cloud compatibility. This requires business to take the lead, not wait for regulators or research bodies to define abstract models.

6. Use Public Procurement to Incentivise Market-Driven Standards

Governments should design cloud tenders to favour open, interoperable solutions that align with widely adopted standards. This creates real demand signals for providers. Schemes like EUCS must be designed to reflect market-led practices, not theoretical compliance checklists. Public procurement should amplify what works in the market not invent parallel requirements.[68]

7. Legal Clarity to Enable Voluntary Business Collaboration

One barrier to business-led standardisation is fear of breaching antitrust rules. The EU should issue guidance or soft law to clarify when joint development of APIs or interoperability layers is permissible. Without such clarity, companies will hesitate to cooperate even when collaboration is pro-competitive and innovation-enhancing.

8. Prioritise Standards for Commercially Relevant Interoperability

Not all services need uniform standards. A risk-based approach should prioritise core functions like IAM, workload orchestration, and data transfer areas where fragmentation harms portability and user control. Standardising niche, performance-sensitive workloads may add complexity without real benefit. Again, business use cases should determine priorities.

---

[67] See, e.g., ISO (2025). Directives and policies. Available at https://www.iso.org/directives-and-policies.html. The ISO/IEC Directives define the basic procedures to be followed in the development of International Standards and other publications. Also see IEEE (2025). Operations Manuals and Bylaws. Available at https://standards.ieee.org/about/policies/. For instance, a good model is the CEN-CENELEC Guide 29:2024 on Workshop Agreements (CWAs), which supports fast-track, consensus-driven technical specifications tailored to emerging needs. CWAs preserve flexibility, promote interoperability, and are well-suited to complex, rapidly evolving sectors like cloud computing. CENELEC (2024). CEN- CENELEC GUIDE 29. Available at https://www.cencenelec.eu/media/Guides/CEN-CLC/cenclcguide29.pdf. ISO Standard. https://www.iso.org/standard/66639.html.

[68] European Commission (2022). An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0031.

9. Promote Global Coherence Through Business-Led Dialogue

Cloud markets are global. European businesses must play a proactive role in international standards bodies (e.g. ISO/IEC JTC 1) and work with counterparts in the US and Asia. Business diplomacy not regulatory extraterritoriality is key to shaping a coherent global standards environment.[69]

6. CONCLUSION AND POLICY RECOMMENDATIONS

Europe's ambition to lead in cloud and AI depends on its ability to translate policy objectives into real customer choice. Cloud customer choice, the freedom to select, combine, and switch providers without undue restrictions is not only critical to innovation and competition, but also to ensuring public sector resilience and digital sovereignty.

While cloud customer choice is not the sole driver of digital transformation, this report demonstrates that enhancing it could unlock up to €1.2 trillion in additional EU GDP by 2030, with particularly strong gains in lagging Member States and the public sector. Crucially, unlocking broader multi-cloud adoption in public administrations, a direct outcome of stronger cloud customer choice could generate up to €450 billion per year in fiscal savings and productivity gains.

Yet the continued presence of fragmented regulatory frameworks, restrictive licensing conditions, and insufficient interoperability mechanisms significantly constrains the adoption, portability, and effective integration of cloud and AI technologies within Europe's digital economy.

To address these challenges, we propose a dual strategy:

- **Short-Term Opportunities** – targeted actions to reduce friction, clarify rules, and support voluntary cooperation.
- **Long-Term Necessities** – structural reforms to regulation, standardisation, and enforcement aligned with openness and competition.

6.1 Competition Authorities

Short-Term Opportunities

- **Encourage structured cooperation:** Use soft law and guidance to support pro-competitive collaboration, particularly in emerging areas such as AI deployment and data portability.
- **Prioritise case-by-case enforcement against anti-competitive lock-in practices,** including discriminatory licensing, bundling, and self-preferencing especially in markets and behaviours that fall outside the scope of the DMA. To avoid duplication and legal fragmentation, there should be a clearer institutional and

[69] See, e.g. ISO/JTC1/IEC (2025). ISO and IEC Joint Technical Committee (JTC 1) for information technology, is a consensus-based, voluntary international standards group. Available at https://jtc1info.org.

procedural separation between DMA enforcement and traditional EU and national competition law.
- **Clarify legal boundaries for technical cooperation:** Provide EU-level guidance under Article 101 TFEU on when firms may align APIs, collaborate on reference architectures, or share interoperability protocols without breaching competition rules. This would reduce the chilling effect on voluntary, market-driven standards and support greater customer choice.

Long-Term Necessities

- **Maintain scrutiny of systemic lock-in risks:** Keep antitrust oversight of software–infrastructure tie-ins, and licensing models that may limit customer mobility across services and markets.
- **Recognise the role of proprietary and open-source models in global innovation diffusion:** Expand competition assessments to better reflect how both proprietary and open-source technologies contribute to innovation, scalability, and cross-border technology diffusion. Proprietary service integration is not inherently anti-competitive and can enable rapid deployment and user adoption. Enforcement should focus on conduct and market effects – not on business models per se – to ensure that competition policy remains supportive of innovation-led growth in dynamic cloud and AI markets.
- **Support pro-competitive standard-setting:** Encourage structured antitrust safe harbours for cloud and AI consortia developing voluntary, industry-led standards. Provide legal certainty for pro-competitive collaboration, especially where interoperability challenges require shared reference models or joint technical specifications.

6.2 Standard-Setting Bodies (SSOs)

Short-Term Opportunities

- **Accelerate delivery of practical, implementation-ready standards:** Prioritise fast-track mechanisms such as CEN-CENELEC Workshop Agreements (CWAs) and ISO Publicly Available Specifications (PAS) to develop standards for workload portability, identity federation, and orchestration.
- **Facilitate structured engagement with open-source projects:** Create formal liaison frameworks between SSOs and key open-source communities (e.g. CNCF, Linus Foundation Europe) to co-develop portable specifications based on existing tools (e.g. Kubernetes, Cilium).
- **Provide practical FRAND guidance through positive and negative lists:** Deliver short-term, service-specific guidance on how FRAND principles apply in cloud and AI markets. This includes defining positive lists (e.g., widely used licensing terms for software integration) where FRAND obligations should apply, and negative lists (e.g. proprietary integrations, custom AI models) where they should not. As outlined

in this report, such clarity would reduce legal uncertainty, minimise disputes, and promote interoperability without penalising innovation.

Long-Term Necessities

- **Institutionalise FRAND guidance and integrate it into global frameworks:** Building on short-term service-level guidance, standard-setting bodies should embed structured FRAND principles into formal governance processes and global standardisation models. This includes formalising positive and negative lists through industry consensus, aligning them with regulatory frameworks, and integrating them into international cooperation efforts (e.g. ISO/IEC JTC 1). Over time, this approach can provide a stable reference point for global cloud and AI service interoperability and licensing across jurisdictions.
- **Coordinate globally:** Deepen engagement in ISO/IEC JTC 1 and other international fora to ensure that European technology standardisation efforts align with global frameworks. Promote mutual recognition of technical specifications, joint reference models, and open market access to avoid fragmentation and to scale European digital competitiveness globally.

6.3 Regulators (EU Policymakers and National Governments)

Short-Term Opportunities

- **Leverage procurement to drive openness**: Embed non-discriminatory licence portability and multi-cloud compatibility in cloud tenders. Public procurement should prioritise vendor-neutral and interoperable solutions as a default.
- **Support SME and open-source participation in standards development:** Provide targeted funding to enable underrepresented businesses to contribute to technical and governance workstreams, ensuring inclusive outcomes.
- **Issue non-binding guidance on FRAND-compatible contractual practices:** Rather than introducing new regulation, regulators should develop practical guidance on contractual clauses that support fair, reasonable, and non-discriminatory (FRAND-like) licensing for cloud and AI services. This could include recommended terms for licence portability and clarification of practices that may be inconsistent with openness or interoperability. Such guidance would help reduce legal ambiguity, support voluntary standardisation, and provide a reference point for both public procurement and private contracting.

Long-Term Necessities

- **Reform digital regulation to target actual harms:** Recalibrate the Data Act, Digital Markets Act, and upcoming proposals like the Digital Networks Act and Cloud/AI

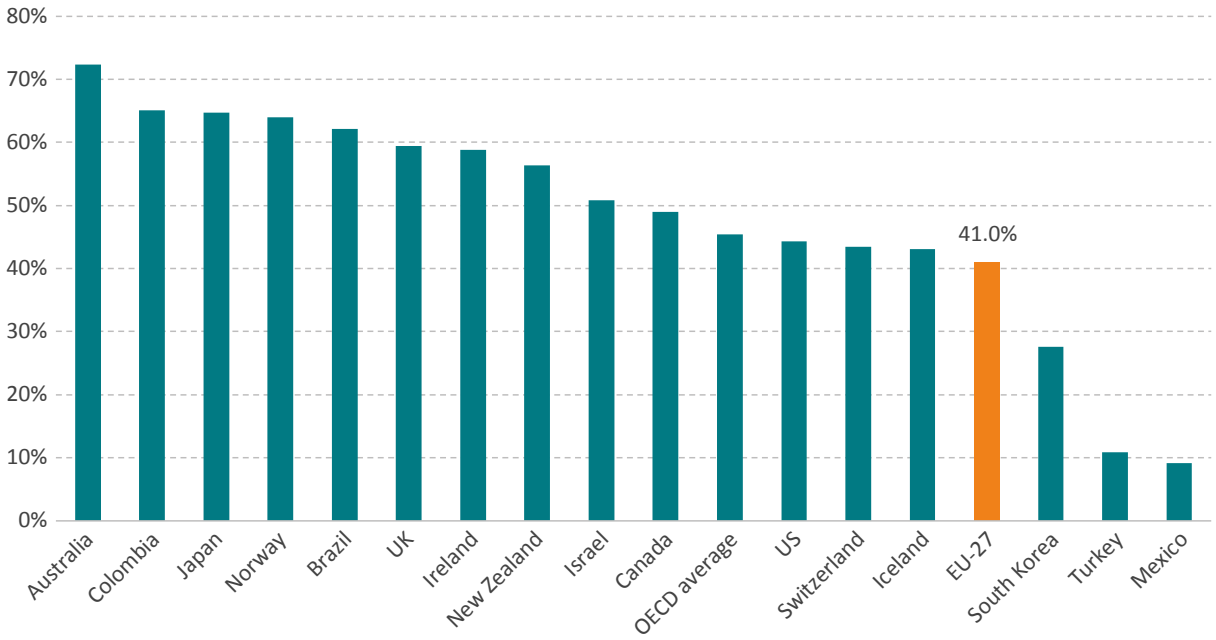
Development Act to avoid rigid mandates and architectural prescriptions. Prioritise case-by-case competition enforcement grounded in market evidence.

- **Advocate sovereignty through user freedom:** Redefine digital sovereignty not as a preference for national suppliers, but as a commitment to user agency, resilience, and openness. Ensure access to global technologies within verifiable, standards-based governance frameworks.
- **Modernise public sector capabilities and procurement:** Upgrade IT governance and procurement in Member States to support multi-cloud-by-default policies and interoperable digital public services. These reforms alone could unlock up to €450 billion in annual public sector efficiency gains.

Cloud customer choice is not a secondary objective, it is a strategic enabler of Europe's digital competitiveness, innovation capacity, and public sector resilience. Delivering that choice requires legal clarity, open licensing frameworks, and standards that reflect real-world deployments. Europe must shift from controlling cloud architecture to enabling dynamic ecosystems where users choose, providers compete, and innovation flourishes.

ANNEX I: SUPPLEMENTARY DATA TABLES ON EU CLOUD UPTAKE AND ADOPTION

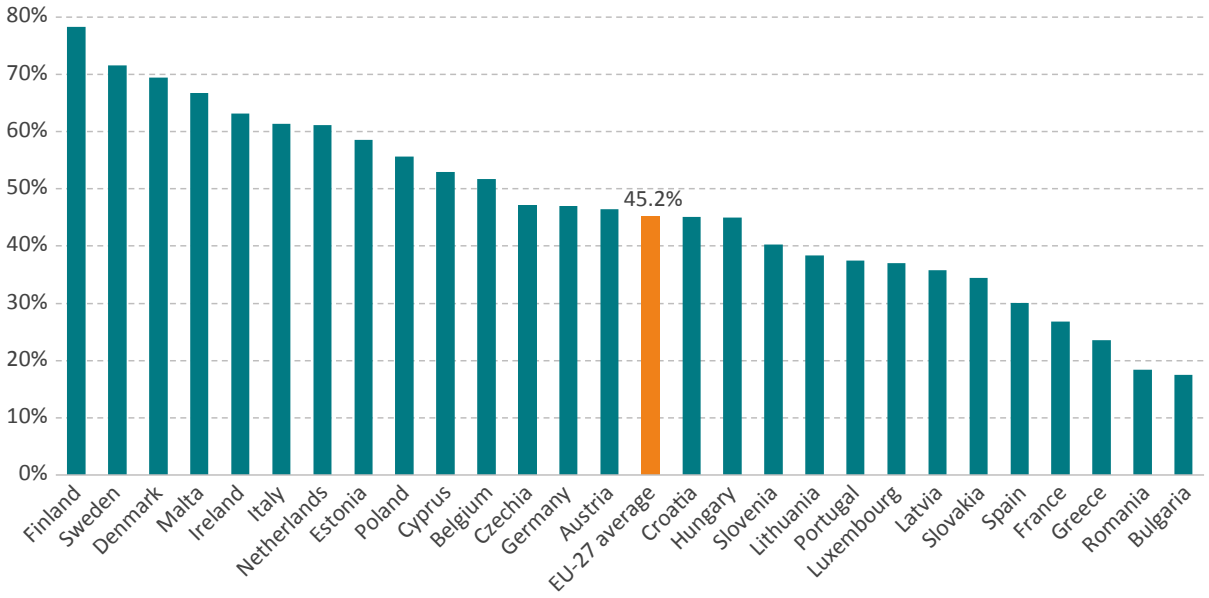
FIGURE 3: SHARE OF BUSINESSES PURCHASING CLOUD SERVICES IN THE EU-27 AND SELECTED GLOBAL ECONOMIES, 2022 OR LATEST AVAILABLE YEAR (PERCENTAGE OF ALL BUSINESSES)



Source: ECIPE elaboration based on OECD Going Digital Toolkit[70] data. Note: All available countries were included in the chart, except for individual EU-27 Member States. The notion of "all businesses" refers to firms with 10 or more employees, excluding those in the financial sector.

[70] OECD. (2022). Businesses purchasing cloud computing services (%). Going Digital Toolkit. Available at https://www.oecd.org/going-digital-toolkit.

FIGURE 4: SHARE OF BUSINESSES PURCHASING CLOUD SERVICES AMONG EU-27 MEMBER STATES, 2023 (PERCENTAGE OF ALL BUSINESSES)



Source: ECIPE elaboration based on Eurostat data. Beyond cross-country variation, other factors help to explain the EU's lag in cloud adoption compared to its international peers. One important element is the difference in cloud uptake across economic sectors. Table 1 sheds light on this dimension, offering a comparison with the OECD average.

TABLE 10: SHARE OF BUSINESSES PURCHASING CLOUD SERVICES BY SECTOR IN THE EU-27 AND OECD, 2021 (PERCENTAGE OF ALL BUSINESSES)

Sector	EU-27	OECD	+ / – (%)
Information and communication	76%	74%	2%
Professional, scientific and technical activities	56%	62%	– 10%
Real estate activities	48%	52%	– 7%
Wholesale trade, except of motor vehicles and motorcycles	47%	50%	– 7%
Administrative and support service activities	41%	46%	– 10%
Manufacturing	40%	44%	– 11%
Transportation and storage	35%	41%	– 15%
Retail trade, except of motor vehicles and motorcycles	34%	37%	– 8%
Construction	32%	38%	– 17%
Accommodation and food and beverage service activities	32%	33%	– 1%
All businesses	**41%**	**45%**	**– 10%**

Source: ECIPE elaboration based on OECD Going Digital Toolkit data. Note: The notion of "all businesses" refers to firms with 10 or more employees, excluding those in the financial sector.

TABLE 11: SHARE OF BUSINESSES PURCHASING CLOUD SERVICES BY FIRM SIZE IN THE EU-27 AND OECD, 2021 (PERCENTAGE OF ALL BUSINESSES)

Firm size	EU-27	OECD	+ / – (%)
Large businesses (250 persons employed or more)	72%	74%	-3%
Medium businesses (50-249 persons employed)	53%	57%	-8%
Small businesses (10-49 persons employed)	38%	42%	-11%
All businesses	**41%**	**45%**	**-10%**

Source: ECIPE elaboration based on OECD Going Digital Toolkit data. Note: The notion of "all businesses" refers to firms with 10 or more employees, excluding those in the financial sector.

ANNEX II: METHODOLOGICAL CONSIDERATIONS – ESTIMATING THE MACRO-ECONOMIC IMPACT OF CLOUD AND AI ADOPTION IN THE EU27

This methodology is inspired by recent country-level studies, which focused on estimating the economic contribution of increased cloud computing adoption to national productivity and GDP, using a combination of digital adoption rates, sectoral value added, and assumed productivity multipliers.[71] While these studies concentrate exclusively on the effects of cloud computing, our approach extends the scope to include automation and AI technologies, applying a similar logic and structure.[72]

This analysis estimates the potential combined (cloud and cloud-based AI) macroeconomic impact – measured as increases in gross value added (GVA) – resulting from increased adoption of cloud computing and AI/automation technologies across the EU27.

Geographic and Sectoral Scope

The model covers all 27 EU Member States and applies the NACE Rev.2 sector classification to distinguish twelve core sectors:

- Agriculture, forestry and fishing
- Industry (excluding construction)
- Manufacturing
- Construction
- Wholesale, retail, transport, accommodation, and food services
- Information and communication
- Financial and insurance activities
- Real estate activities
- Professional, scientific, technical and administrative services
- Public administration, defence, education, health and social work
- Arts, entertainment, other services, households, and extra-territorial bodies

[71] Teleadvisors (2024). Economic Impact of Cloud Computing in the United Kingdom. Available at https://www.teleadvs.com/reports-3/. Also see Teleadvisors (2024). Economic Impact of Cloud Computing in Germany, Amazon Web Services. Available at https://www.teleadvs.com/reports-3/.

[72] For a study on AI, see Teleadvisors (2024). Economic impact of Cloud Computing and Artificial Intelligence in Europe. Available at https://www.teleadvs.com/economic-impact-of-cloud-computing-and-artificial-intelligence/. Although this study does not provide an aggregate GDP effect, cloud computing – and, to a lesser extent, AI – are accounted for as productivity-enhancing inputs in a structural production model. The authors estimate that a 1% increase in cloud adoption is associated with a 0.135% rise in gross value added (GVA), rising to 0.178% when AI adoption is above the median. While results are expressed in GVA, they approximate GDP effects at the sectoral level, highlighting the significant economic gains that could result from closing Europe's cloud and AI adoption gap.

Key Data Sources

1. **Gross Value Added (GVA):** Eurostat [nama_10_a10__custom_16526215], current prices, million euro
2. **Digital Intensity Index (DII):** Share of enterprises with very low, low, high, or very high digital intensity (Version 4)
3. **Cloud Adoption Rates:** Percentage of enterprises using cloud computing services (Eurostat, 2023)
4. **AI Adoption Rates:** Percentage of enterprises using one or more AI technologies (Eurostat, 2024)

Analytical Framework

Step 1 – Weighting Sectoral GVA by Digital Intensity

- Sector-level GVA is adjusted using digital intensity shares, with each bracket assigned a weight to reflect its readiness to benefit from technology adoption (Note: digital intensity shares reflect: share of enterprises with very low, low, high, or very high digital intensity):

Digital Intensity Level	Weight
Very low	0.2
Low	0.4
High	0.6
Very high	0.8

These weights account for the differential ability of sectors to translate technology inputs into productivity gains.

Step 2 – Estimating Technology-Driven Productivity Gains

- Cloud adoption: Cloud computing primarily enables infrastructure efficiency and IT cost reduction by shifting storage, processing, and workflows from on-premise systems to scalable cloud environments. These benefits tend to materialise relatively quickly after adoption – as upfront investments translate into operational savings – and thus are treated as one-off gains that plateau once migration is complete. Accordingly, we assume these gains are realised in full during the scenario period and remain stable thereafter.
- AI and automation: In contrast, AI adoption supports ongoing, dynamic productivity improvements by augmenting human decision-making, automating tasks, and enabling new forms of service delivery. These gains accumulate over time as organisations refine models, expand use cases, and embed AI more deeply in

operations. Therefore, we model AI-driven gains as cumulative and compounding, reflecting their long-term contribution to productivity growth.

- No inter-sectoral spillovers, displacement effects, or capital/labour reallocation dynamics are modelled explicitly.
- Cloud computing: A one-off productivity gain of 2.24% is applied across digital-intensity-weighted GVA, based on firm-level data from Germany and the UK. These gains reflect measurable improvements in operational efficiency, ICT flexibility, and cost structures following cloud adoption.
- To quantify the potential productivity impact, we reference a recent McKinsey impact assessment that explores the economic benefits of deploying generative AI and other advanced technologies. According to this analysis, the automation of individual work activities through these technologies could boost global productivity by 0.5% to 3.4% annually from 2023 to 2040, depending on the rate of automation adoption.[73] Of this growth, generative AI alone is projected to contribute 0.1 to 0.6 percentage points, provided that individuals impacted by these technologies transition to other work activities that maintain or enhance their productivity levels.
- Applying the conservative estimate of a 1.7% annual productivity improvement, we calculate the potential gains from the adoption of cloud-based AI solutions within the public sector. This includes the integration of generative AI and automation technologies. We incorporate productivity growth estimates to illustrate long-term cumulative effects, applying McKinsey's projections of a 5.2% increase over 3 years and 10.6% over 6 years. Even with low cloud adoption, AI-driven productivity gains – particularly through automation – can significantly accumulate, enhancing government functions.

Step 3 – Defining Adoption Scenarios

Scenario 1 – Ambitious Adoption

- Cloud adoption: Each sector in each Member State is assumed to reach the current EU27 sectoral maximum. For countries that already exhibit maximum values (e.g. Estonia, Denmark, Sweden, depending on the sector and whether cloud or AI is considered), adoption rates are assumed to increase by an additional 10% – a deliberately conservative estimate.
- AI adoption: Adoption increases to the maximum observed rate per sector across the EU. For countries that already exhibit maximum values (e.g. Estonia, Denmark, Sweden, depending on the sector and whether cloud or AI is considered), adoption rates are assumed to increase by an additional 10% – a deliberately conservative estimate.

[73] McKinsey (2023). The economic potential of generative AI. The next productivity frontier. Available at https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2023/2023-06-14%20mgi%20genai%20report%2023/the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf

Scenario 2 – Less Ambitious Adoption

- Cloud and AI adoption: In each sector and country, adoption increases by 50% of the gap between current levels and the EU sectoral maximum.

Step 4 – Modelling GVA Uplift

For each scenario, productivity gains are calculated as: GVA × Digital Intensity Weight × Productivity Gain × Projected Adoption Increase

This yields both:

- Absolute gains (in million euro), and
- Relative gains (as a percentage of baseline GVA)

Results of Economic Modelling:

TABLE 12: CHANGES IN GDP BY SCENARIO

Country/ region	Changes in GDP - Scenario 1 - Ambitious Cloud and AI Adoption, long-term (6Y)	Changes in GDP - Scenario 1 - Ambitious Cloud and AI Adoption, short-term (3Y)	Changes in GDP - Scenario 2 - Less Ambitious Cloud and AI Adoption, long-term (6Y)	Changes in GDP - Scenario 2 - Less Ambitious Cloud and AI Adoption, short-term (3Y)
EU27	7.3%	3.6%	4.0%	2.0%
Belgium	2.1%	1.1%	1.4%	0.7%
Bulgaria	22.8%	11.2%	12.9%	6.3%
Czechia	11.5%	5.6%	6.1%	3.0%
Denmark	1.6%	0.8%	1.1%	0.6%
Germany	4.2%	2.1%	2.5%	1.3%
Estonia	6.1%	3.1%	3.2%	1.6%
Ireland	4.9%	2.4%	2.6%	1.3%
Greece	9.3%	4.6%	5.2%	2.6%
Spain	11.2%	5.5%	6.4%	3.2%
France	12.1%	6.0%	6.9%	3.4%
Croatia	8.3%	4.1%	4.5%	2.2%
Italy	12.5%	6.2%	6.4%	3.2%
Cyprus	18.4%	9.0%	9.4%	4.6%
Latvia	11.7%	5.7%	6.3%	3.1%
Lithuania	13.0%	6.4%	7.0%	3.5%

Country/ region	Changes in GDP - Scenario 1 - Ambitious Cloud and AI Adoption, long-term (6Y)	Changes in GDP - Scenario 1 - Ambitious Cloud and AI Adoption, short-term (3Y)	Changes in GDP - Scenario 2 - Less Ambitious Cloud and AI Adoption, long-term (6Y)	Changes in GDP - Scenario 2 - Less Ambitious Cloud and AI Adoption, short-term (3Y)
Luxembourg	2.6%	1.3%	1.8%	0.9%
Hungary	17.6%	8.6%	9.1%	4.5%
Malta	5.7%	2.9%	3.0%	1.5%
Netherlands	2.4%	1.2%	1.4%	0.7%
Austria	3.3%	1.6%	2.0%	1.0%
Poland	20.8%	10.2%	10.6%	5.2%
Portugal	14.4%	7.1%	7.9%	3.9%
Romania	32.4%	15.9%	17.7%	8.7%
Slovenia	5.4%	2.7%	3.2%	1.6%
Slovakia	10.4%	5.1%	5.9%	2.9%
Finland	1.8%	0.9%	1.1%	0.6%
Sweden	2.0%	1.0%	1.2%	0.6%

Source: ECIPE estimation.

ANNEX III: METHODOLOGICAL CONSIDERATIONS REGARDING THE INTERPRETATION AND ROBUSTNESS OF ESTIMATED IMPACTS

This economic assessment uses a structured modelling approach to estimate the potential productivity and output gains from increased cloud and AI adoption across EU Member States and sectors. The methodology draws on sectoral gross value added (GVA) data and applies adoption elasticities informed by recent empirical studies. It distinguishes between one-off efficiency gains associated with cloud migration and the cumulative productivity effects of AI and automation.

While the model captures key channels through which digital technologies impact economic performance including cost savings, process efficiencies, and labour productivity improvements it necessarily relies on simplifying assumptions and proxy indicators. Most notably, it assumes that each sector in each country can feasibly reach the current EU maximum level of cloud or AI adoption. For countries that already meet or exceed this benchmark, a conservative 10% additional increase is applied. Cloud-related gains are modelled as static, front-loaded effects, while AI-driven gains are treated as dynamic and compounding over time.

A core limitation is the lack of granular, harmonised data on the actual depth and quality of cloud and AI use across sectors. Available adoption rates do not reflect functional integration, strategic deployment, or organisational maturity factors which significantly influence the realised impact of these technologies. Moreover, while the applied elasticities are grounded in the latest econometric literature, they are generalised across countries and sectors and may not fully reflect national institutional conditions, regulatory barriers, or labour market frictions.

The model does not account for second-order effects such as demand spillovers, innovation complementarities, or dynamic behavioural responses by firms. Nor does it estimate transition costs or frictions, including skills mismatches, integration of legacy IT, or slow-moving procurement systems in the public sector. In addition, the modelling applies uniform productivity multipliers without adjusting for variations in digital readiness, automation potential, or capital-labour substitution elasticity across sectors.

Importantly, these figures should be interpreted as indicative. For countries starting from a very low base, projected gains may appear unrealistically high within a six-year horizon. However, the underlying message remains valid: there is substantial room for productivity enhancement – not only in the private sector, but especially in the public sector, where cloud and AI technologies remain significantly underutilised.

Crucially, the estimated gains are not forecasts. They represent stylised scenarios designed to illustrate the opportunity cost of continued under-adoption and the potential economic upside of enabling policies. Actual outcomes will depend on Member States' implementation pace, investment in digital skills, regulatory openness, and institutional commitment to transformation.

The modelling approach also adopts a deliberately conservative stance. It limits projected gains to near-term, technologically achievable improvements based on current use cases. While the analysis does not formally distinguish between "thin" and "thick" adoption due to data limitations, this conceptual distinction remains useful. Thin adoption refers to basic or isolated use of cloud and AI technologies (e.g. online storage or basic automation), whereas thick adoption entails strategic, integrated use across entire operations – enabling new production models, improved service delivery, and innovation.

Because most of the available data reflects thin or early-stage adoption, the estimates presented here largely capture the effects of modest, incremental uptake. However, if firms and public institutions move rapidly towards thick adoption and if structural barriers such as vendor lock-in, procurement fragmentation, or skills gaps are addressed the actual economic gains could substantially exceed the baseline scenarios outlined in this report.