ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

TOWARDS COMPETITIVE CLOUD ECOSYSTEMS

Strategic Responses for Europe's Digital Future

JUDITH ARNAL

JULY 2025

TABLE OF CONTENTS

ABSTRACT

Cloud computing has become the foundational infrastructure for Europe's digital transformation, yet market concentration and vendor lock-in practices are undermining the continent's capacity to compete. This paper examines the fundamental relationship between competition and competitiveness in cloud markets, where effective competition among providers is not merely desirable but a precondition for European economic competitiveness.

Three key findings emerge from this mixed-method analysis combining literature review, regulatory assessment, and expert consultation. First, while the EU's Data Act and Digital Markets Act represent genuine regulatory innovation, implementation gaps and fragmented enforcement threaten their effectiveness. Second, market leaders are evolving their business models in response to regulatory developments, with software licensing emerging as an increasingly important competitive dimension that merits closer regulatory and supervisory attention. Third, strategic assessment reveals tensions between regulatory ambitions and structural market realities.

WE PROPOSE A THREE-PILLAR POLICY RESPONSE:

Strengthening competition law enforcement to address evolving software licensing practices under Articles 101 and 102 TFEU;

Closing regulatory gaps through extended oversight of software licensing and enhanced interoperability standards;

Leveraging strategic public procurement to shape market dynamics and support emerging European providers.

I.
INTRODUCTION:
CLOUD, COMPETITIVENESS AND COMPETITION

Cloud computing refers to the remote provision of computing resources—such as storage, processing power, and applications—delivered via the internet by third-party providers. By eliminating the need to own and maintain physical IT infrastructure, it allows firms and public administrations to scale operations flexibly, reduce costs, and access cutting-edge digital tools.

As such, cloud computing, which is widely recognized as an enabling technology, has become the foundational infrastructure for AI, big data, and other key digital innovations. Their strategic relevance extends beyond IT departments: they shape firms' capacity to innovate, adapt, and compete in increasingly digitalized markets.[1]

The adoption of public cloud computing has been shown to boost productivity and firm size through several mechanisms, including cost savings, enhanced operational flexibility, and improved worker efficiency.[2] Moreover, the falling price of cloud services has further facilitated their uptake: the nominal price of a selected class of cloud products fell by 58% between the first quarter of 2010 and the third quarter of 2018.[3] When adjusting for quality improvements, the effective price decline reaches approximately 80%.

Without access to cloud resources, many firms, especially SMEs[4], would be unable to afford the infrastructure required to experiment, test, and deploy these new tools[5]. By turning capital expenditures into operating expenses, businesses gain flexibility and can redirect resources toward innovation and customer service.

For public sector institutions, cloud computing contributes to improving service delivery, security, data management, sustainability, and administrative efficiency. By leveraging cloud platforms, governments can enhance the quality and speed of digital public services, ensure more robust disaster recovery systems, and strengthen inter-agency data sharing. These improvements can be particularly significant in healthcare, education, and social protection systems. In addition, cloud solutions can help governments reduce IT maintenance costs, improve cybersecurity, and comply with evolving data governance requirements.

Despite the recognized benefits of cloud computing, its adoption in the EU lags behind the US and Asia. Indeed, according to Gartner, cloud adoption in the US has reached an impressive 60%, highlighting a high level of integration. In contrast, European companies are making progress but still lag behind, with adoption rates around 41%.[6]

There are substantial disparities in cloud adoption across EU Member States. In 2023, in countries like Finland (78.3%), Sweden (71.6%), Denmark (69.5%), and Malta (66.7%), more than 65% of enterprises bought cloud computing services. In contrast, adoption remains below 25% in Greece (23.6%), Romania (18.4%), and Bulgaria (17.5%). Spain stood below the EU average, at 30%.

Several interrelated factors contribute to the lagging adoption of cloud in the EU, encompassing technical, organizational, and market dynamics.[7]

First, the availability of human capital is a key constraint. Large firms report difficulties in hiring and retaining skilled ICT professionals as one of the most significant barriers to adopting advanced digital technologies such as cloud computing and big data.[8] This challenge is particularly acute in sectors with low digital maturity or limited access to specialized labor markets.

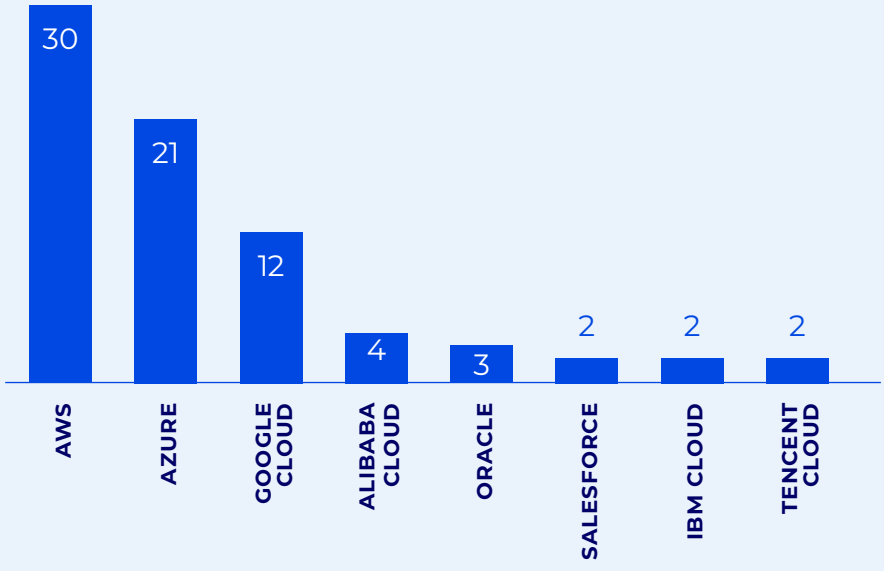
Second, concerns over data privacy, security, and localization continue to deter organizations from migrating to the cloud.[9] Surveys have consistently found that firms worry about the protection of sensitive information and the location of data servers, especially in the absence of a harmonized data privacy regime across jurisdictions.[10]

Third—and central to this paper—is the concern about vendor lock-in and lack of effective competition. Firms often encounter technical and contractual difficulties in switching cloud providers, including non-interoperable application programming interfaces (APIs), proprietary data formats, and restrictive contractual terms. These potential obstacles may increase switching costs and create dependencies that can stifle innovation, inflate costs, and reduce user trust. These frictions inhibit contestability in the cloud services market.[11] Market dynamics in the cloud infrastructure sector reveal a striking degree of provider dominance. A small number of firms command the vast majority of global market share, pointing to limited competition in a foundational segment of the digital economy. As illustrated in Figure 1, such concentration raises concerns about potential market power, reduced contestability, and dependency risks—all of which directly affect competitiveness, innovation and security across sectors.

Figure 1.
Global market share of leading cloud infrastructure service providers in Q4 2024*.

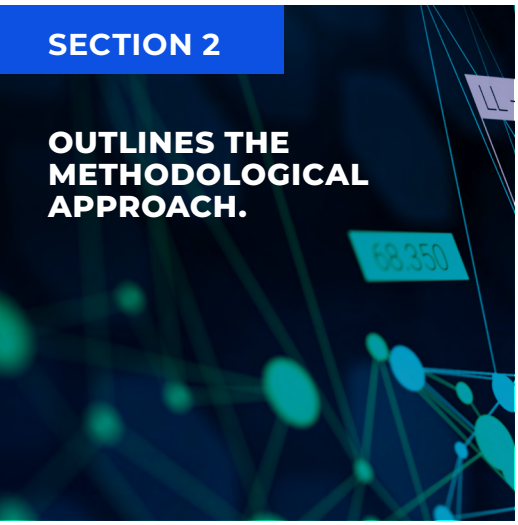
Source:
Own elaboration based on data from Synergy Research Group and Statista

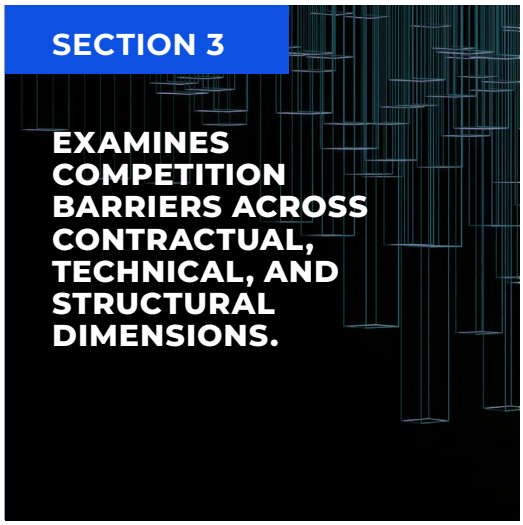
**Includes platform as a service (PaaS) and infrastructure as a service (IaaS), as well as hosted private cloud services.*

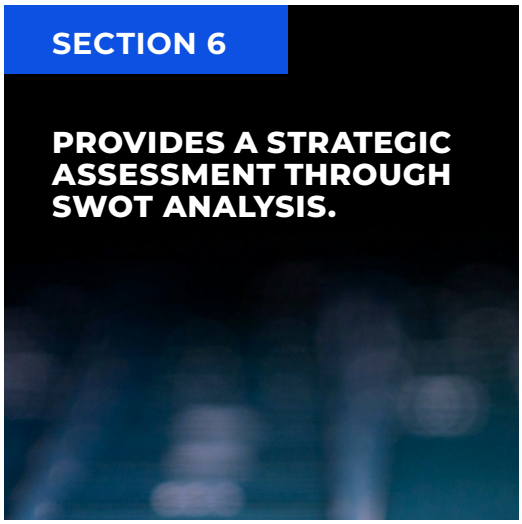


While competitiveness and competition are conceptually distinct[12]—the former referring to a firm's or economy's ability to compete effectively in the market, and the latter to the structure and functioning of markets—in the case of cloud computing, the two notions converge. A lack of competition among cloud providers impedes freedom of choice, limits service quality, innovation, and pricing efficiency, which in turn constrains firms' ability to benefit from cloud-enabled productivity gains. Moreover, high switching costs and weak contestability act as barriers to cloud adoption itself,[13] thereby reducing digital competitiveness at both firm and macroeconomic level. **In this specific technological domain, competition is a precondition for competitiveness.**

The analysis proceeds as follows:







2. METHODOLOGICAL APPROACH

This foresight brief employs a mixed-method qualitative approach combining systematic literature review with expert consultation to examine governance challenges and policy responses in EU cloud computing markets.

The analysis draws on academic and institutional literature across three domains: competition economics in digital markets, regulatory governance scholarship, and policy implementation studies.

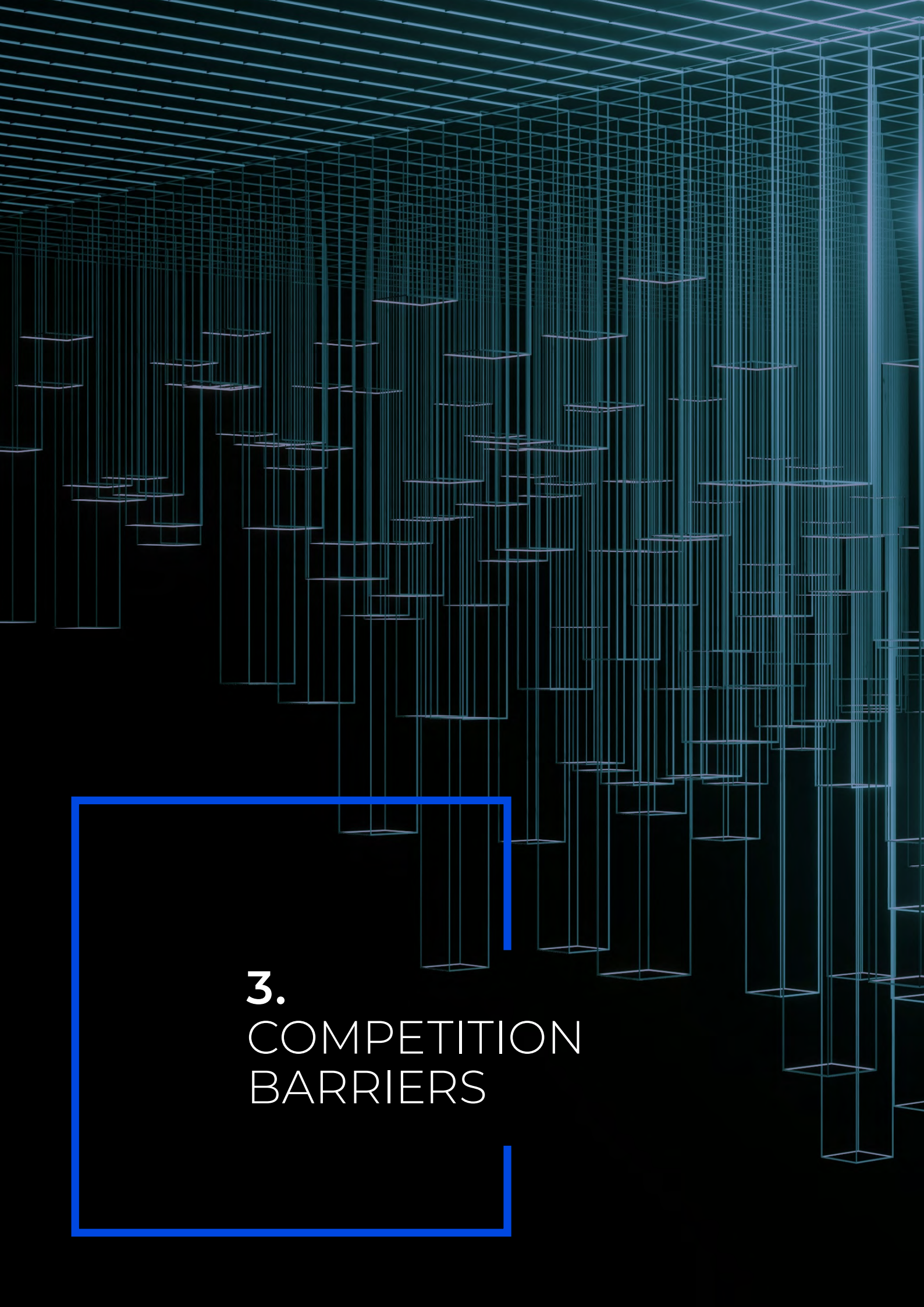
To validate desk research findings, a structured consultation session was conducted with stakeholders from the public sector, including competition authorities, academia and private industry at IE University in May 2025.

The analysis employs a barrier typology classifying potential competitive restrictions by their economic nature (contractual, technical, strategic, structural) and regulatory addressability (ex ante rules, ex post enforcement, market-based solutions).

Several limitations should be acknowledged:

- temporal constraints limit empirical evidence on Data Act implementation,
- stakeholder selection may under-represent SME perspectives, and
- the dynamic nature of cloud markets means findings may be affected by technological changes.

Despite these limitations, the combination of literature review, regulatory analysis, and expert validation provides a robust foundation for understanding current governance challenges and assessing policy responses.



3. COMPETITION BARRIERS

This section examines the barriers that hinder effective competition in cloud markets. These barriers—contractual, technical, strategic, and structural—reflect the diverse ways in which market frictions manifest and interact. While each category presents distinct challenges, their combined effect reinforces incumbency advantages, limits user choice, and reduces the contestability that is essential for a dynamic and competitive cloud ecosystem.

3.1. CONTRACTUAL INCENTIVES LIMITING CUSTOMER CHOICE

One of the main obstacles to effective competition in cloud computing markets lies in the structure of contractual incentives that restrict mobility and lock customers into long-term relationships with dominant providers. These contractual arrangements, often invisible to end users, can create significant economic frictions that deter switching and multi-provider strategies. Among the most prominent mechanisms are data egress fees, cloud credits, and committed spend agreements.

Data egress fees refer to charges imposed by cloud providers when customers transfer their data out of the provider's environment to another service or to on-premises infrastructure. While ingress—uploading data to the cloud—is typically free or low-cost, the asymmetric pricing of data egress can create a strong financial disincentive to exit.[14] High egress fees have been criticized for significantly raising the cost of migrating to alternative cloud providers, particularly for users managing large-scale datasets. These charges can lead customers to stay with their current provider not due to superior service or competitive pricing, but because of artificially inflated switching costs.[15] Empirical evidence shows that, when large volumes of data are involved, such fees can account for a non-negligible share of total IT expenditures.[16]

Cloud credits are another contractual tool frequently used by major providers to attract and retain customers. These are promotional or usage-based credits offered—often in high amounts—to new customers or startups in exchange for future loyalty or exclusivity.[17] The issue arises when these credits are conditional upon minimum commitments or cannot be transferred across providers. Large-scale credits can generate dependency and delay customers' willingness to evaluate alternative suppliers.[18] This is particularly problematic for smaller firms and startups, which may become locked into specific cloud ecosystems due to the initial attractiveness of "free" capacity.[19] The largest cloud firms can afford to offer substantial credits, thereby reinforcing their market dominance and raising barriers to entry for smaller competitors unable to match such offers.[20]

Committed spend agreements represent a more formalized version of this dynamic. Under these arrangements, clients agree to spend a certain amount—often in the millions of euros or dollars—over a specified period, usually in exchange for discounts or access to premium services.[21] These contracts, while financially attractive in the short term, create high exit costs and long-term dependencies. Customers are disincentivized to diversify their cloud providers or to adopt multi-cloud strategies, since doing so could jeopardize the volume-based benefits or expose them to penalties.[22] As documented in various market inquiries,[23, 24] these agreements particularly affect large public institutions and multinational firms that engage in strategic digital transformation processes.

Collectively, these contractual mechanisms reinforce the advantages of incumbents and inhibit market contestability. They reduce price transparency, restrict client freedom, and ultimately limit the ability of newer or smaller cloud providers to compete on a level playing field. This dynamic has raised concerns not only among European competition authorities but also in the United States, where the Federal Trade Commission has announced an inquiry into how contract structures in cloud computing may distort market outcomes.[25]

Beyond these contractual mechanisms, a related but distinct issue is the skills ecosystem, which operates as a functional barrier to competition. Leading cloud providers increasingly offer large-scale free training programs as part of broader commercial engagements, particularly in the public sector. While presented as capacity-building, these initiatives create implicit incentives for institutions to consolidate their operations on a single platform. Smaller providers, by contrast, are often unable to match the scale or scope of such offers, placing them at a structural disadvantage.

The problem extends further: many training programs are tied to proprietary certifications, and vendor-neutral credentials remain underdeveloped.[26] Some providers have also established partnerships with educational institutions, embedding platform-specific knowledge from early stages of education. Over time, this leads to a cloud and AI talent pool trained on—and professionally dependent upon—a single ecosystem, reinforcing lock-in from the supply side.[27] Certifications issued by dominant providers have become critical career assets, and technical staff often have a vested interest in maintaining the platforms on which they have been trained.

3.2. TECHNICAL BARRIERS TO INTEROPERABILITY AND PORTABILITY

Technical barriers to interoperability and data portability are among the most persistent frictions in cloud computing markets.

> These barriers constrain customers' ability to migrate workloads or data between cloud environments or to operate across multiple providers in parallel.

Unlike contractual lock-in mechanisms, technical restrictions are embedded in the underlying design of cloud systems, from proprietary interfaces to non-standard data schemas and orchestration tools.

Interoperability refers to the capacity of distinct systems and services to work together seamlessly, while portability describes the ease of transferring data and applications across platforms without significant reconfiguration. Although both are conceptually distinct, they are interdependent in practice and essential for dynamic, competitive markets. However, many cloud

services—particularly in Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) segments—are intentionally designed to be closed ecosystems, with limited standardization and high switching costs.[28]

The French competition authority has proposed a useful typology to understand these technical barriers, classifying them by the nature of the transition the user wishes to undertake. The first form of friction emerges when an organization seeks to migrate from an on-premise IT environment to a cloud-based architecture. This shift often requires a complete reengineering of legacy systems, adapting them to virtualized environments, containers, or serverless computing models. Applications must be rewritten or heavily modified to operate within the specific toolsets and configuration protocols of the selected cloud provider. The learning curve, integration effort, and risk of failure are all non-trivial, creating strong lock-in from the very first migration.

The second layer of barriers becomes visible when users consider switching from one cloud provider to another. Despite marketing claims of flexibility, most cloud providers employ proprietary APIs, identity management systems, and storage formats that complicate portability. Incompatible APIs, custom monitoring tools, and divergent security protocols require full reconfiguration and retesting. These technical hurdles make transitions prohibitively expensive or risky, especially for SMEs.

A third level of complexity arises when organizations attempt to implement multi-cloud strategies. While using services from multiple providers can improve resilience and reduce dependency, the reality is that some providers do not facilitate this approach. Resource orchestration, load balancing, and compliance monitoring across heterogeneous clouds require high levels of technical sophistication. In many cases, cloud vendors design their services in ways that discourage cross-provider compatibility. As a result, multi-cloud implementation remains viable only for highly mature organizations with significant engineering capacity.[29]

Importantly, many of these technical obstacles are not inevitable consequences of technological limitations but the result of deliberate architectural choices.

> Indeed, the lack of interoperability in cloud markets often reflects strategic behavior by dominant providers aiming to retain customers through technological enclosure.[30]

This is consistent with earlier patterns in digital markets, where non-compatibility served to entrench dominant positions.

Standardization initiatives—such as those led by ISO, ETSI, and open-source communities—have only partially alleviated these barriers. While containerization technologies like Docker and orchestration tools such as Kubernetes provide a degree of abstraction, they are often insufficient to ensure full interoperability without deep customization. Moreover, vendor-specific extensions of these tools are increasingly common, undermining their standardizing potential.[31] As discussed later in the paper, the forthcoming implementation of the EU Data Act aims to address some of these frictions by establishing binding obligations to improve both portability and interoperability in cloud services.

3.3. STRATEGIC BARRIERS: SOFTWARE LICENSING RESTRICTIONS AND BUNDLING PRACTICES

Beyond contractual and technical barriers, certain commercial strategies related to software licensing and product bundling, by legacy software providers, have raised concerns regarding their potential to limit effective competition in cloud markets.

Restrictive software licensing refers to contractual clauses that condition the use of specific software products to particular cloud infrastructures, or that impose financial or operational penalties when those products are deployed in competing environments.[32] These restrictions may be particularly impactful when associated with widely used productivity suites, databases, or operating systems, where customer dependence is high. The use of "Bring Your Own License" (BYOL) policies—nominally designed to offer flexibility—can in practice be structured to favour in-house cloud environments, thereby reinforcing vendor lock-in.[33] Such licensing terms may lead to effective foreclosure, especially for smaller providers that cannot replicate the same ecosystems or enterprise bundles. Thus, several competition authorities (e.g. US FTC and UK CMA) are paying close attention to this and investigating these practices.

Bundling practices in the cloud context involve the combination of infrastructure, platform, and software services in a single package, often with pricing or performance incentives attached.[34] While bundling can offer efficiency gains, it may also disincentivize users from switching providers or adopting a multi-cloud strategy. Bundling essential middleware with proprietary tools or APIs may distort user choice and raise barriers to entry for specialized service providers. Empirical analyses[35] highlight how bundling in digital markets can entrench incumbents' market power, especially when interoperability is limited.

> Beyond economic costs, these restrictive practices compromise security by forcing customers onto a single platform, creating a dangerous 'monoculture' vulnerability that increases concentration risk. This lock-in can force customers to remain in a cloud environment despite security problems, undermining overall digital resilience.

Large CSPs typically operate at global scale, allowing them to spread fixed costs across a vast user base and invest heavily in innovation, cybersecurity, and energy-efficient infrastructure

3.4. STRUCTURAL ADVANTAGES OF DOMINANT PROVIDERS AND MARKET ENTRY BARRIERS

In addition to contractual and technical restrictions, a set of structural features further consolidate the dominant position of the largest cloud service providers (CSPs), limiting competition and raising entry barriers for smaller firms.

Large CSPs typically operate at global scale, allowing them to spread fixed costs across a vast user base and invest heavily in innovation, cybersecurity, and energy-efficient infrastructure.[36] This scale advantage makes it extremely difficult for new entrants to compete on cost or service quality.[37] Moreover, the largest providers, sometimes, own and operate their own data centers, which enables greater control over latency, redundancy, and compliance with data localization requirements.[38] By contrast, smaller CSPs often rely on colocation or third-party infrastructure, making them dependent on upstream providers and limiting their ability to differentiate.[39]

Vertical integration reinforces these advantages. Many of the leading CSPs offer both infrastructure services (IaaS) and proprietary software or platforms (PaaS, SaaS), often pre-integrated and optimized for in-house use. This tight integration can generate lock-in effects even without explicit contractual barriers, as users become accustomed to proprietary APIs, interfaces, or workflows.[40] Such integration may act as a form of "quasi-tying," especially when interoperability standards are lacking or underdeveloped[41].

Another critical barrier stems from reputational and regulatory asymmetries. Public institutions and highly regulated industries (such as finance and healthcare) may be reluctant to engage with smaller providers due to perceived risks regarding reliability, security, or regulatory compliance.[42]

Finally, network effects also play a role. When cloud providers build extensive partner ecosystems and developer communities, they create technical and human capital lock-ins that are difficult for challengers to replicate.[43] This is particularly evident in environments where skills, certifications, and integrations are tightly coupled with a single provider's architecture.[44]

4. PROGRESS AND NEW BARRIERS

Having identified the contractual, technical, and structural mechanisms that restrict competition in cloud markets, this section turns to the regulatory and enforcement response. Recent EU initiatives seek to correct these failures by lowering switching costs, improving interoperability, and curbing exclusionary behavior. Yet despite notable progress, new forms of strategic adaptation have emerged, revealing persistent asymmetries in regulatory reach. What follows is a critical assessment of both the advances and the limitations of current frameworks, with particular focus on the Data Act, the Digital Markets Act, and the challenges of ex post enforcement under EU competition law.

4.1. REGULATORY ADVANCES: THE DATA ACT AND THE DATA MARKETS ACT

The Data Act and the Digital Markets Act (DMA) represent two complementary initiatives within the EU's digital strategy, both of which seek to address structural inefficiencies and market failures in cloud computing. While the Data Act provides a horizontal regulatory framework designed to enhance data mobility and interoperability,[45] the DMA targets the conduct of dominant digital platforms—classified as "gatekeepers"—with the aim of restoring contestability and mitigating dependency risks in data infrastructure.[46]

The Data Act introduces, for the first time, legally binding obligations for providers of data processing services to remove contractual, commercial, technical, and organizational barriers that impede switching. This is intended to strengthen user control over data and digital assets and to reduce the risk of vendor lock-in, particularly in PaaS and SaaS layers, where proprietary architectures and lack of standardized interfaces often inhibit interoperability. A cornerstone of the Act is the principle of functional equivalence,[47] which requires that migrated services maintain sufficient technical continuity to enable users to operate effectively in alternative environments. This provision, while innovative, raises nontrivial implementation challenges, including the risk of regulatory-induced homogenization: ensuring baseline compatibility across services could inadvertently lead to a lowest-common-denominator outcome, thereby undermining service differentiation and technical innovation.

In operational terms, the regulation mandates a phased elimination of switching fees. From January 2024 to January 2027, providers are only allowed to charge for the direct costs incurred in facilitating migration; beyond that point, all switching-related charges are

prohibited. The goal is to realign economic incentives and remove pricing frictions that deter user mobility. However, enforcing compliance with these provisions will fall under the jurisdiction of national authorities, raising concerns about fragmentation and uneven implementation across Member States.[48] Although penalties of up to 4% of global turnover are foreseen, the deterrent effect will depend on the capacity and willingness of national regulators to act decisively.

Complementing the Data Act, the DMA introduces a set of ex ante obligations for large platforms that control access to essential digital services, including cloud infrastructure.[49] By designating certain firms as gatekeepers based on quantitative thresholds and qualitative criteria, the DMA seeks to curb exclusionary practices such as bundling, self-preferencing, and interoperability restrictions.[50] In the cloud context, this regulatory logic may be particularly relevant given the growing entanglement between cloud services and adjacent software ecosystems.[51] Practices that tie proprietary productivity tools to infrastructure-as-a-service offerings, or that condition interoperability on exclusive terms, fall squarely within the scope of DMA enforcement. Although with divergent views among actors, the DMA thus could provide an additional layer of regulatory oversight aimed at neutralizing structural sources of dependency that the Data Act alone may not fully address.

Together, these two instruments could constitute a dual-track regulatory approach: the Data Act seeks to create technical and contractual conditions for fair switching, while the DMA addresses the market behavior of dominant providers that could undermine those conditions. Their effectiveness, however, hinges on the development of robust interoperability standards, the availability of open interfaces, and the alignment of enforcement strategies across Member States. Without sustained coordination at both technical and political levels, there is a risk that regulatory ambition may not translate into tangible market outcomes.

Moreover, **while both instruments mark significant progress, key gaps remain**. The Data Act's provisions on egress fees do not account for the full range of switching costs, which often include costly application re-architecture, penalties from long-term commercial agreements, and the need to retrain technical teams. These frictions can accumulate and undermine effective user mobility, particularly for large organizations managing complex digital environments. On the DMA side, although the regulatory framework provides mechanisms to address exclusionary behavior in cloud markets, no cloud infrastructure provider has yet been formally designated as a gatekeeper. As a result, the potential of the DMA to address structural dependencies in cloud computing remains, for now, largely theoretical. Ensuring that these tools evolve in step with market realities will be essential to realizing their intended impact.

The Data Act seeks to create technical and contractual conditions for fair switching, while the DMA addresses the market behavior of dominant providers that could undermine those conditions

4.2. THE LIMITS OF EX POST ENFORCEMENT: ARTICLES 101 AND 102 TFEU

In addition to the ex ante provisions introduced by the Data Act and the DMA, EU competition law provides ex post instruments to address exclusionary conduct in cloud markets, notably through Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU). These provisions, while legally robust, face important limitations when applied to fast-moving digital markets.

Article 101 TFEU prohibits agreements between undertakings that restrict competition, including collusive arrangements or vertical contracts that foreclose market access. In the cloud context, this could encompass exclusive licensing agreements or contractual terms that limit interoperability or portability across providers. Article 102 TFEU prohibits the abuse of a dominant position, and has been interpreted to include bundling, tying, discriminatory pricing, and loyalty-inducing rebates—all of which may be relevant to cloud business models. However, the enforcement of these provisions is inherently reactive and case-specific. Competition authorities must demonstrate actual or potential foreclosure effects through detailed economic analysis, access to internal firm data, and well-defined market boundaries—requirements that are particularly difficult to satisfy in complex, layered digital markets.[52] Moreover, legal uncertainty and the duration of investigations often reduce the deterrent effect of enforcement actions.

As a result, while Articles 101 and 102 TFEU remain essential components of the regulatory toolkit, they are insufficient on their own to address the evolving dynamics of cloud-based market power.[53] Their limited ability to anticipate strategic adaptation by dominant firms highlights the need for a complementary, more dynamic framework.[54]

4.3. STRATEGIC ADAPTATION: SOFTWARE LICENSING AS A POST-REGULATORY LOCK-IN MECHANISM

Faced with regulatory constraints on contractual switching terms and data portability, some incumbent providers appear to be reinforcing control through the licensing perimeter, where the regulation remains silent.[55]

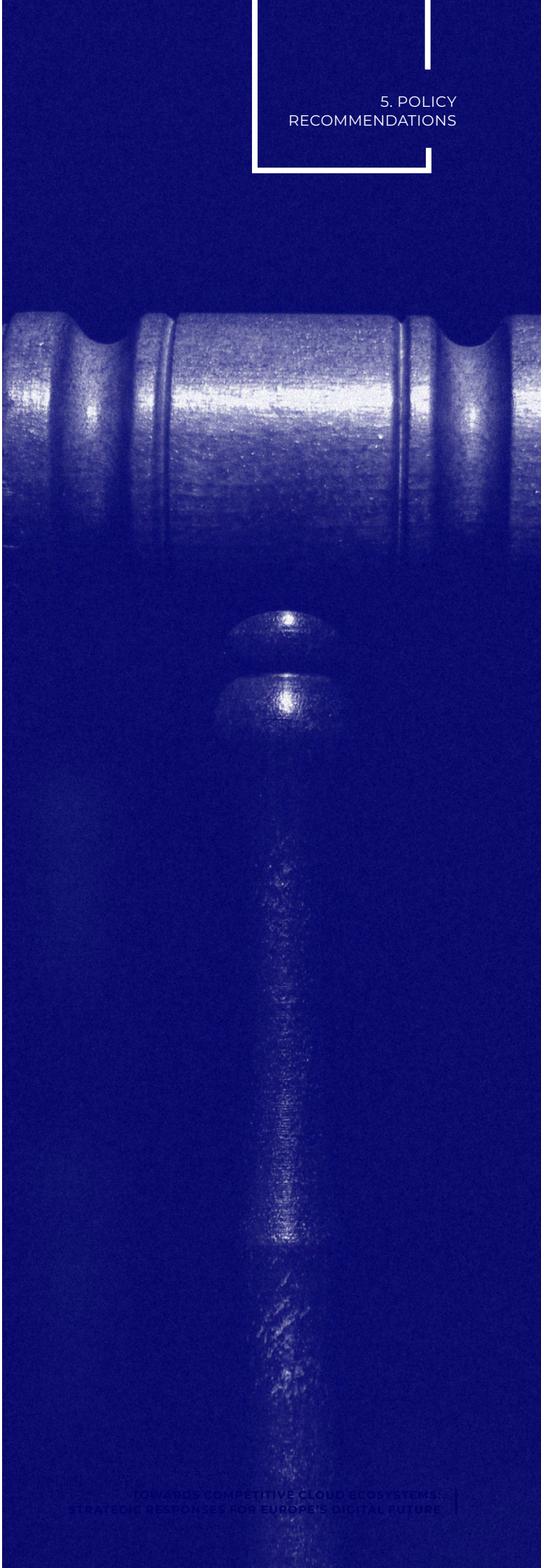
This strategic adaptation underscores a broader regulatory asymmetry: while the Data Act imposes obligations on cloud service providers to enhance interoperability and switching at the cloud service layer, it does not directly address upstream software licensing practices that are critical for cloud-based operations. As a result, providers may comply formally with interoperability rules while introducing licensing conditions that limit the practical implementation of multi-cloud strategies, potentially leading to continued customer lock-in.

> These dynamics raise complex questions about the boundary between legitimate commercial differentiation and conduct that may hinder competition.

From a legal standpoint, certain behavior could, in some circumstances, fall within the scope of Article 102 TFEU if they result in abuse of dominance.[56] Yet enforcement tends to be reactive and context-dependent, and many practices remain in a gray zone where competitive effects are difficult to assess in real time.[57]

This underscores the importance of a more adaptative and forward-looking regulatory framework—one that accounts for the ways in which market power can shift across different layers of the digital infrastructure stack and ensures coherence in its intervention perimeter.

5. POLICY RECOMMENDATIONS



5.1. STRENGTHENING COMPETITION LAW ENFORCEMENT TO ADDRESS EVOLVING MARKET PRACTICES

Given the limits of ex ante regulation and the reactive nature of ex post enforcement, competition authorities must adopt a more dynamic and anticipatory approach to evolving forms of market power in cloud computing.[58] As described in section 4.2, Articles 101 and 102 TFEU remain critical tools, but their application in layered, fast-moving markets requires renewed institutional capacity, better access to technical and contractual data, and refined analytical methods.

In particular, the growing role of software licensing as a mechanism for strategic adaptation (see section 4.3) demands closer scrutiny under Article 102 TFEU.

> Practices such as tying cloud infrastructure to proprietary licenses, conditioning interoperability on exclusivity clauses, or imposing loyalty-inducing terms in volume contracts can amount to exclusionary abuse if they generate significant foreclosure effects.

National authorities and the European Commission should prioritize investigations that examine how such licensing strategies undermine multi-cloud feasibility and user choice.

At the same time, Article 101 TFEU must be applied not only to traditional collusive conduct, but also to vertical agreements that limit effective competition through opaque or restrictive licensing clauses. Particular attention should be paid to agreements between dominant cloud providers and software vendors that restrict the use of software across cloud environments or foreclose rivals by way of bundled incentives.

5.2. CLOSING REGULATORY GAPS: LICENSING, INTEROPERABILITY AND GOVERNANCE

While the Data Act and the DMA represent landmark steps in European digital regulation, their effectiveness in fostering cloud competition depends on comprehensive alignment across all dimensions of the cloud competition. As shown in section 4.3, the licensing layer—particularly the structuring of software access and BYOL restrictions—has become an increasingly important component of cloud service delivery models. Ensuring coherent coverage of this layer within existing regulatory frameworks represents an opportunity to maximize policy effectiveness and market outcomes.

To optimize regulatory coherence, policymakers could benefit from recognizing how licensing structures interact with data portability and interoperability objectives, ensuring that all elements of the cloud stack work harmoniously to support user choice and market dynamism. In this context, collaborative industry initiatives—such as voluntary standardized contract clauses, industry-developed codes of conduct, and multi-stakeholder interoperability frameworks—could provide innovative and flexible solutions that complement existing regulations while preserving competitive differentiation. These instruments should be developed through inclusive dialogue with industry leaders, SMEs, and public sector customers to ensure both market relevance and practical implementation.

Strengthened governance through public-private partnership will also play a key role. The success of the Data Act's switching provisions will benefit from proactive collaboration between regulators and industry stakeholders in developing implementation best practices. Therefore, the creation of a dedicated European oversight body—working in close cooperation with industry to promote cloud interoperability, advance licensing transparency, and enhance contractual clarity—merits consideration as a collaborative governance model that supports both innovation and competition. This oversight function becomes even more relevant in light of the structural gaps discussed above. While the Data Act does not address the full spectrum of switching frictions, and the DMA has not yet designated any cloud infrastructure provider as a gatekeeper, the persistence of systemic barriers calls for continuous regulatory monitoring. A dedicated body could play a crucial role in identifying blind spots, coordinating enforcement approaches, and issuing soft law guidance to ensure coherence across legal instruments. Without such a function, fragmentation and regulatory inertia risk undermining the EU's broader digital policy goals.

> Finally, given the limitations identified in current legislative instruments, it is essential to ensure that the EU's digital rulebook remains responsive to emerging challenges.

In particular, where systemic barriers to switching fall beyond the scope of the Data Act, and where cloud infrastructure providers are not captured under current gatekeeper designations in the DMA, existing tools should be implemented effectively and used to their full potential. In addition, policymakers may consider leveraging supplementary instruments—such as sector-specific guidance, soft law mechanisms, or delegated powers to competent authorities—to address residual exclusionary practices in a timely and proportionate manner. Such an approach would enhance the adaptability of the regulatory framework and help translate regulatory ambition into genuinely competitive market conditions.

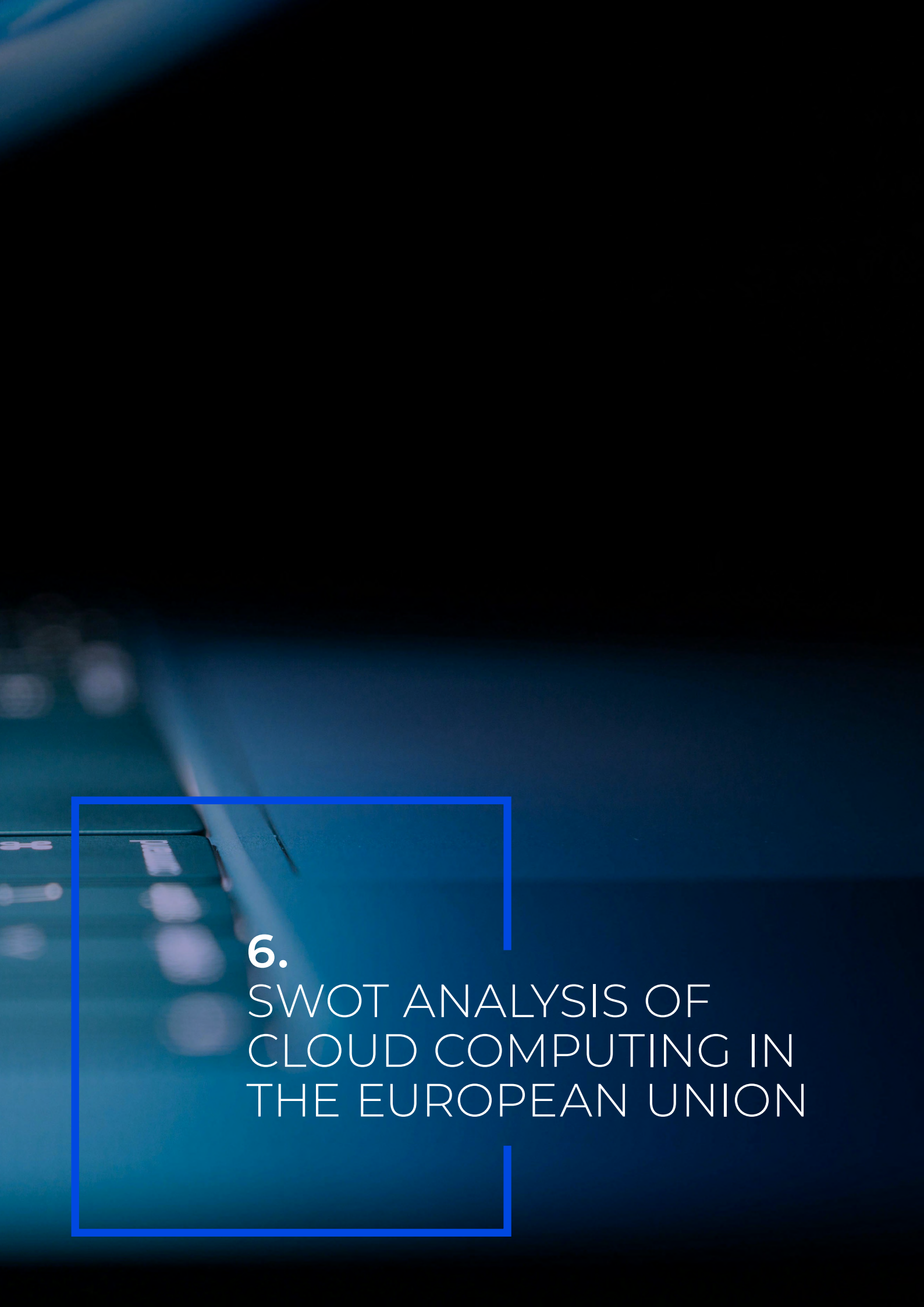
5.3. LEVERAGING PUBLIC PROCUREMENT FOR CLOUD ADOPTION AND COMPETITIVE RESILIENCE

Public procurement can play a transformative role in fostering a more open and competitive cloud services market in the EU. To unlock this potential, structural reforms should ensure that procurement practices actively support market contestability and technological resilience. Tender specifications should promote transparency systematically include requirements for interoperability, reversibility, sustainability, and multi-cloud compatibility, while evaluation criteria must go beyond price to reward openness, vendor-neutral architectures, and technical robustness (incl. security robustness). These elements are essential to prevent long-term dependency and ensure that public investment contributes to a dynamic and diversified ecosystem. Moreover, reversibility should go beyond generic lists of tools or vague exit provisions: public tenders should require fully costed exit plans, at least in the form of indicative estimates, so that buyers understand the total cost of ownership, including potential disengagement scenarios. This would help mitigate the underestimated financial and operational impact of switching providers.

In support of this, the European Commission should develop model contract clauses and technical guidelines that help public buyers incorporate pro-competitive principles into the design and execution of cloud tenders. This effort should build on the 2025 guide by the Spanish competition authority (CNMC) on the preparation and design of public tenders.[59] While not specific to cloud/IT, the guide includes valuable recommendations to avoid anti-competitive practices such as excessive bundling or supplier lock-in, and to promote fair and open participation. Drawing on this and complementary work by national digital agencies, the Commission should provide practical templates addressing common lock-in risks—such as egress fees, proprietary formats, or bundled services—and ensure that their use is mandatory across all relevant procurement frameworks. Optional adoption risks being circumvented, especially in procedures that allow direct awards or where suppliers' standard terms are accepted by default. Effective enforcement mechanisms and monitoring are necessary to prevent erosion of these safeguards in practice.

At the same time, structural barriers within public finance frameworks must be addressed. One major obstacle is the CAPEX/OPEX asymmetry in the accounting treatment of cloud spending. While cloud services are typically classified as operational expenditure (OPEX), most public budgeting systems continue to favor capital expenditure (CAPEX). This creates a disincentive for cloud adoption, as OPEX must often be approved annually and lacks the long-term visibility associated with capital investment. Both the OECD and the European Court of Auditors have flagged this issue, calling for reforms to budgeting rules and cost allocation models. Aligning fiscal incentives with the pay-as-you-go nature of cloud services is essential to advance digital transformation objectives across the EU.

Finally, capacity-building within public administrations is essential. Procurement officers often lack the technical and legal expertise to evaluate cloud proposals, assess lock-in risks, or enforce interoperability clauses. Programs under the Digital Europe initiative and national digitalization strategies should include dedicated training modules on cloud procurement, as well as shared platforms for knowledge exchange among public buyers. Yet training alone is not enough. In practice, cloud purchasing decisions are often taken by technical staff deploying services, rather than by professional procurement officials. This shift in decision-making authority can weaken accountability and sideline formal safeguards. To address this, governments should promote blended teams that bring together legal, commercial, and technical expertise. Only through multidisciplinary collaboration can public administrations ensure effective oversight, avoid unintended lock-in, and align procurement with long-term digital policy goals.



6.
SWOT ANALYSIS OF CLOUD COMPUTING IN THE EUROPEAN UNION

The EU stands at a critical juncture in cloud computing governance. This section provides a systematic assessment of the EU's strategic position, identifying internal capabilities and external dynamics that will shape the effectiveness of cloud governance in the coming decade, as summarized below.

STRENGTHS (INTERNAL)

First-mover advantage with the Data Act, introducing binding data portability and switching rights.

Sophisticated dual-track regulatory architecture (Data Act + DMA).

Large public sector demand base gives leverage via procurement.

Strong competition law enforcement tradition and ongoing national inquiries.

WEAKNESSES (INTERNAL)

Fragmented implementation across Member States; varying enforcement capacity and expertise.

Procurement and administrative capacity gaps, especially in evaluating interoperability and lock-in.

Market concentration with no EU cloud provider playing a relevant role; strategic and autonomy vulnerabilities.

Slow competition enforcement; reactive nature of TFEU Articles 101 and 102.

OPPORTUNITIES (EXTERNAL)

Rising demand for multi-cloud and interoperability driven by customer experience.

Edge computing, containerization, and cloud-native architectures enable competition.

Momentum for digital sovereignty and EU-aligned cloud ecosystems.

European advantage in AI and privacy could support sector-specific, competitive offerings.

THREATS (INTERNAL)

Market consolidation: emergence of "super clouds" may make switching infeasible.

Strategic adaptation by dominant providers through licensing practices that circumvent regulation.

Global regulatory fragmentation may lead to legal uncertainty and favour incumbents.

Geopolitical risks: service disruptions or access restrictions from international tensions.

6.1. INTERNAL STRENGTHS: REGULATORY INNOVATION AND MARKET FOUNDATIONS

The EU's cloud governance approach combines regulatory innovation, strategic leverage, and institutional depth, positioning it as a potential global standard-setter. The EU's dual-track strategy—merging sector-specific rules (Data Act) with platform regulation (DMA)—addresses both technical and behavioral barriers in layered digital markets. Additionally, the EU's market power, especially via public procurement, enhances its influence over global providers. Finally, recent national competition investigations are building a solid empirical foundation for future regulatory action.

6.2. INTERNAL WEAKNESSES: IMPLEMENTATION GAPS AND COORDINATION CHALLENGES

Despite its regulatory ambition, the EU faces key internal weaknesses that threaten the effectiveness of its cloud governance. Fragmented implementation across Member States leads to uneven enforcement and risks regulatory arbitrage. A capacity gap, especially in public procurement, limits the ability of institutions to evaluate interoperability or prevent lock-in, while accounting rules further disincentivize cloud adoption.

Market concentration with no EU cloud provider playing a relevant role poses risks to both competition and strategic autonomy, as European actors remain dependent on foreign-controlled infrastructure. Additionally, slow and reactive enforcement mechanisms, such as under Articles 101 and 102 TFEU, struggle to keep pace with fast-evolving digital markets, reducing their deterrent power.

6.3. EXTERNAL OPPORTUNITIES: MARKET DYNAMICS AND TECHNOLOGICAL SHIFTS

Several external trends offer strategic openings to strengthen EU cloud governance. Rising enterprise concerns over vendor lock-in—driven by outages, security incidents, and pricing disputes—have increased demand for multi-cloud and interoperability, aligning market sentiment with regulatory goals. Technological shifts like edge computing, containerization, and cloud-native architectures enhance portability and reduce monopolistic tendencies, while tools like Kubernetes support more open ecosystems.

Geopolitical tensions and the push for digital sovereignty have elevated support for European cloud alternatives and stricter interoperability rules. The growing importance of AI workloads also introduces new competitive dynamics, where Europe's strength in industrial AI and data protection may offer an edge. Lastly, public sector digitalization, accelerated post-pandemic, creates a major opportunity for European providers—if procurement policies prioritize openness and competition.

6.4. EXTERNAL THREATS: MARKET CONSOLIDATION AND STRATEGIC ADAPTATION

The EU's cloud governance strategy faces major external threats that could weaken its effectiveness and strategic autonomy. Market consolidation and the rise of tightly integrated "super clouds" risk making interoperability impractical and raising entry barriers. Dominant providers' strategic adaptations, such as using software licensing to maintain lock-in, exploit regulatory gaps across legal domains, challenging enforcement.

Global regulatory fragmentation may lead to conflicting frameworks, increasing complexity and favoring incumbents. Potential clashes—such as between EU interoperability rules and US IP protections—could create legal uncertainty. Finally, the geopolitical weaponization of cloud infrastructure introduces systemic risks, including service disruptions and data access conflicts, which may simultaneously boost demand for EU alternatives while complicating global cooperation.

7. CONCLUSIONS

This analysis has explored the governance challenges in European cloud computing, highlighting the crucial link between competition and competitiveness. Cloud services are foundational for AI, data-driven innovation, and productivity, but their transformative potential is hindered by market concentration and barriers to adoption stemming from weak competition. Effective competition is thus not only a regulatory aim but essential for Europe's digital competitiveness.

Three key insights emerge.

First, the EU has shown global leadership through innovative frameworks like the Data Act and DMA, advancing data portability and platform accountability. Yet, implementation remains fragmented and constrained by limited administrative capacity and technical expertise, threatening their impact.

Second, market power in cloud ecosystems is highly adaptive. As traditional lock-in practices are curbed, dominant providers have shifted to subtler exclusionary strategies—such as software licensing restrictions—exploiting regulatory blind spots. This underscores the need for agile, anticipatory governance.

Third, despite its regulatory leverage, the EU faces structural challenges in global cloud markets. Realizing a more open ecosystem requires bridging implementation gaps and enhancing coordination and institutional responsiveness.

Going forward, aligning regulatory innovation with enforcement capacity is vital. Addressing licensing-related lock-in is an urgent task, and broader institutional reforms are needed to stay ahead of incumbents' strategic adaptations. Without effective competition, Europe risks a cycle of low cloud adoption and limited productivity gains. The EU's approach, if successfully implemented, could set a global standard—but its success is a strategic imperative, not just a regulatory choice.

ENDNOTES

1 Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

2 Andrews, D., Nicoletti, G., & Timiliotis, C. (2018). *Digital technology diffusion: A matter of capabilities, incentives or both?* OECD Economics Department Working Papers, No. 1476. OECD Publishing. https://doi.org/10.1787/7c542c16-en

3 Byrne, D. M., Corrado, C., & Sichel, D. E. (2018). The rise of cloud computing: *Minding your P's, Q's and K's*. In C. Corrado, J. Miranda, J. Haskel & D. Jorgenson (Eds.), *Measuring and Accounting for Innovation in the Twenty-First Century* (pp. 213–240). University of Chicago Press. https://doi.org/10.7208/chicago/9780226734801.003.0006

4 OECD. (2021). *The digital transformation of SMEs*. OECD Studies on SMEs and Entrepreneurship. OECD Publishing. https://doi.org/10.1787/bdb9256a-en

5 OECD. (2022). Cloud computing and competition. OECD Digital Economy Papers, No. 331. https://doi.org/10.1787/1ba94aab-en

6 Gervais, H. (2025). *The shocking truth behind US-EU productivity gap*. Urbest. https://urbest.io/blog/the-shocking-truth-behind-us-eu-productivity-gap/

7 Anderton, R., Jarvis, V., Labhard, V., Morgan, J., Petroulakis, F., & Vivian, L. (2020). *Virtually everywhere? Digitalisation and the euro area and EU economies* (Occasional Paper Series No. 244). European Central Bank. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op244~2acc4f0b4e.en.pdf

8 European Commission. (2023). *Europe's Digital Decade: digital targets for 2030.* https://digital-strategy.ec.europa.eu/en/policies/digital-decade

9 Berry, D. M., & Reisman, M. (2012). Policy issues in cloud computing: A look at cloud computing adoption across sectors. *International Journal of Technoethics*, 3(2), 35–47.

10 CFO. (2012). *CFO Insights: Cloud Computing.*

11 OECD. (2021). *Barriers to entry, expansion and exit in cloud services.* OECD Competition Committee. https://www.oecd.org/daf/competition/barriers-cloud-services-2021.pdf

12 Porter, M. E. (1990). *The competitive advantage of nations*. Free Press.

13 Crémer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition policy for the digital era. European Commission.* https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

14 Competition and Markets Authority (CMA). (2023). Provisional findings report: Cloud services market investigation.

15 Autorité de la Concurrence. (2023). Avis n° 23-A-05 relatif au fonctionnement concurrentiel du secteur du cloud.

16 Satariano, A. (2022). Cloud Lock-In Costs: Barriers to Data Portability. Journal of Digital Infrastructure Policy, 6(1), 45–62

17 Buyya, R., Yeo, C. S., & Venugopal, S. (2008). *Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities.* arXiv preprint arXiv:0808.3558. https://arxiv.org/abs/0808.3558

18 Competition and Markets Authority (CMA). (2023). Provisional findings report: Cloud services market investigation.

19 Luong, N. C., Wang, P., Niyato, D., Wang, Y., & Han, Z. (2017). *Resource Management in Cloud Networking Using Economic Analysis and Pricing Models: A Survey*. arXiv preprint arXiv:1701.01963. https://arxiv.org/abs/1701.01963

20 Autorité de la concurrence. (2023). *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector.* https://www.autoritedelaconcurrence.fr/sites/default/files/2023-06/Resume_Avis_Cloud%20EN_final_2023_2906.pdf

21 Bergemann, D., & Deb, R. (2025). *Robust pricing for cloud computing.* arXiv preprint arXiv:2502.07168. https://arxiv.org/abs/2502.07168

22 Beslic, I. (2023). *Vendor lock-in and its impact on cloud computing migration* (Master's thesis). DIVA Portal. https://www.diva-portal.org/smash/get/diva2:1787688/FULLTEXT01.pdf

23 Competition and Markets Authority (CMA). (2023). Provisional findings report: Cloud services market investigation.

24 Autorité de la concurrence. (2023). *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector.* https://www.autoritedelaconcurrence.fr/sites/default/files/2023-06/Resume_Avis_Cloud%20EN_final_2023_2906.pdf

25 Federal Trade Commission (FTC). (2023). Cloud computing and competition: Market inquiry notice.

26 Infosec. (n.d.). Decoding IT and cybersecurity certifications: Vendor-specific vs vendor-neutral. https://www.infosecinstitute.com/resources/professional-development/vendor-specific-versus-vendor-neutral-certifications/

27 Computer Weekly. (n.d.). IT talent trap: How cloud skills suffer as a result of supplier lock-in. https://www.computerweekly.com/feature/IT-talent-trap-How-clouds-skills-suffer-as-a-result-of-supplier-lock-in

28 OECD. (2021). Barriers to Entry and Regulation in Cloud Computing. Paris: OECD Digital Economy Papers, No. 311

29 Weyer, E., & Willcocks, L. (2023). European Cloud Sovereignty and the Limits of Interoperability: Lessons from Gaia-X. Journal of Strategic Information Systems, 32(1), 101710

30 Kretschmer, T., & Schneider, P. (2022). Interoperability and Market Power in Digital Ecosystems. Industrial and Corporate Change, 31(4), 789–812. https://doi.org/10.1093/icc/dtac019

31 European Commission. (2023). Study on Cloud Switching and Porting. Brussels: European Commission, DG Connect

32 Competition and Markets Authority. (2025). *Cloud services market investigation: provisional findings.* https://www.gov.uk/guidance/cloud-services-market-investigation-provisional-findings

33 Alhosban, A., Pesingu, S., & Kalyanam, K. (2024). CVL: A Cloud Vendor Lock-In Prediction Framework. *Mathematics, 12*(3), 387. https://doi.org/10.3390/math12030387

34 Autorité de la concurrence. (2023). *Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector.* https://www.autoritedelaconcurrence.fr/sites/default/files/2023-06/Resume_Avis_Cloud%20EN_final_2023_2906.pdf

35 Crémer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition policy for the digital era. European Commission.* https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

36 OECD. (2025). *Competition in the provision of cloud computing services—Background note* (DAF/COMP(2025)8). https://one.oecd.org/document/DAF/COMP(2025)8/en/pdf

37 European Commission. (2022). *Sector inquiry on cloud infrastructure services—Final report.*

38 IBM. (2024). *What is a hyperscale data center?* https://www.ibm.com/think/topics/hyperscale-data-center

39 US Signal. (2023). *Understanding the key differences between data center and colocation: Which is right for your business?* https://ussignal.com/blog/understanding-the-key-differences-between-data-center-and-colocation-which-is-right-for-your-business

40 Ayem, G. T., Thandekkattu, S. G., & Vajjhala, N. R. (2022). Review of interoperability issues influencing acceptance and adoption of cloud computing technology by consumers. En V. S. Reddy et al. (Eds.), *Intelligent Systems and Sustainable Computing* (pp. 49–58). Springer. https://doi.org/10.1007/978-981-19-0011-2_5

41 Loutas, N., Kamateri, E., Bosi, F., & Tarabanis, K. (2011). Cloud computing interoperability: The state of play. *Proceedings of the 1st International Conference on Cloud Computing and Services Science,* 23–33. https://www.researchgate.net/publication/221276685_Cloud_Computing_Interoperability_The_State_of_Play

42 Elena, G., & Johnson, C. W. (2015). Factors influencing risk acceptance of Cloud Computing services in the UK Government. *arXiv preprint arXiv:1509.06533.* https://arxiv.org/abs/1509.06533

43 Si, W. (2024). *Mapping Partnerships in the Global Cloud Platform Ecosystem.* https://www.lse.ac.uk/media-and-communications/assets/documents/research/msc-dissertations/2024/Weizhong-Si-Finalized.pdf

44 Teixeira, J. A., & Hyrynsalmi, S. (2018). How do software ecosystems co-evolve? A view from OpenStack and beyond. a*rXiv preprint arXiv:1808.06663.* https://arxiv.org/abs/1808.06663

45 Ennis, S., & Evans, B. (2023). *Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence.* https://ueaeprints.uea.ac.uk/id/document/172671

46 Hacker, P., Cordes, J., & Rochon, J. (2022). *Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and beyond.* https://arxiv.org/abs/2212.04997

47 Law-Now. (2023). *EU Data Act—Focus on Cloud Services: what is "functional equivalence" and is it necessary?.* CMS Law-Now. https://cms-lawnow.com/en/ealerts/2023/02/eu-data-act-focus-on-cloud-services-what-is-functional-equivalence-and-is-it-necessary

48 Arnal J. (2025). AI at Risk in the EU: It's Not Regulation, It's Implementation. *European Journal of Risk Regulation.* Published online 2025:1-10. doi:10.1017/err.2025.19

49 Carugati, F. (2023). *The Competitive Relationship Between Cloud Computing and Software Markets.* Bruegel Working Paper 19/2023. https://www.bruegel.org/system/files/2023-12/WP%202023%2019%20Cloud%20111223.pdf

50 European Parliament. (2021). *Digital Markets Act: Ensuring fair and open digital markets.* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS_BRI(2021)690589_EN.pdf

51 CERRE. (2022). *Interoperability in Digital Markets.* Centre on Regulation in Europe. https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf

52 Caffarra, C., & Scott Morton, F. (2021). *Understanding the economics of digital ecosystems.* In M. Peitz & M. Reisinger (Eds.), The Economics of Platforms: Concepts and Strategy (pp. 321–348). CEPR Press

53 Lianos, I., & Ivanov, A. (2023). *Regulating ecosystems: Competition law as a tool of digital industrial policy.* CLES Research Paper Series.

54 Khan, L. M. (2019). The Separation of Platforms and Commerce. *Columbia Law Review, 119*(4), 973–1098

55 Kindelán Gómez, A., & Camacho Lázaro, M. (2024). Cloud competition and software licensing: The EU antitrust outlook. *Revista de Derecho de la Competencia y la Distribución,* 41(2), 55–78

56 Whish, R., & Bailey, D. (2021). *Competition Law* (10th ed.). Oxford: Oxford University Press.

57 Petit, N. (2020). B*ig Tech and the Digital Economy: The Moligopoly Scenario.* Oxford: Oxford University Press

58 Petit, N., Teece, D., Innovating Big Tech firms and competition policy: favoring dynamic over static competition, *Industrial and Corporate Change*, Volume 30, Issue 5, October 2021, Pages 1168–1198, https://doi.org/10.1093/icc/dtab049

59 Comisión Nacional de los Mercados y la Competencia. (2025). *Guía sobre la preparación y diseño de las licitaciones públicas (G-2023-01).*

IE UNIVERSITY

CENTER FOR THE GOVERNANCE OF CHANGE

WRITTEN BY:
Judith Arnal

RECOMMENDED CITATION:
Arnal, J. (2025). *Towards Competitive Cloud Ecosystems: Strategic Responses for Europe's Digital Future*, IE Center for the Governance of Change.

IE CGC, July 2025

Photos: Unsplash, Shutterstock
Design: epoqstudio.com

cgc.ie.edu