ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

POLICY PAPER
JUNE 2026

The DMA meets the cloud:

Gatekeepers and beyond

cgc.ie.edu

TABLE OF CONTENTS

AUTHOR:
Laura Zoboli

cgc.ie.edu

This report was prepared for the Center for the Governance of Change (CGC) at IE University. It draws on three sources:
(i) academic and policy literature on cloud computing regulation and competition;
(ii) institutional and regulatory materials, including market studies, enforcement decisions, and legislative texts; and
(iii) a closed-door working breakfast convened by the CGC on April 13, 2026, which brought together nineteen participants[1] from government, regulatory authorities, industry, law firms, and academia.

The discussion was conducted under the Chatham House Rule. Where the report refers to perspectives expressed during the working breakfast, it does so without attribution to individual participants. The analysis and recommendations are the author's own.

1. INTRODUCTION: THE CLOUD–DMA QUESTION

> In November 2025, the European Commission opened three market investigations into cloud computing services under the Digital Markets Act (DMA), marking a significant step in the application of the framework to a sector long subject to sustained policy and regulatory debate.[2]

Two would assess whether Amazon Web Services (AWS) and Microsoft Azure qualify for gatekeeper designation on a qualitative basis. A third would evaluate whether the DMA's existing obligations are adequate for cloud markets at all. The proceedings coincide with the broader review of the DMA under Article 53, published on April 28, 2026, which confirms the overall functioning of the DMA framework while identifying cloud computing services as an area requiring further assessment.[3] Together, they mark a turning point—not only for cloud, but for the DMA's capacity to address forms of market power that differ from those it was originally designed to capture.

The central question at the working breakfast hosted by the CGC on April 13, 2026, was straightforward in formulation but increasingly complex in substance: how should cloud markets be approached within the framework of the DMA?

At a formal level, the answer appears clear. Cloud computing services are included among core platform services under the DMA. Yet, in practice, no cloud provider has been designated as a gatekeeper. This gap between legal inclusion and practical application reflects a deeper tension between the regulatory logic of the DMA and the economic characteristics of cloud computing. The DMA is built around a model of market power centered on intermediation between business users and end users. By contrast, cloud computing is more accurately characterized by vertically integrated architectures, business-to-business relationships, and forms of dependency that do not rely on direct intermediation.

This tension emerged repeatedly in the discussion. Several participants highlighted the difficulty of applying user-based designation criteria to cloud markets, where economic relevance derives from enterprise-scale dependency rather than large user bases. Others emphasized that, despite these conceptual challenges, cloud markets exhibit features—including concentration, switching barriers, and ecosystem integration—that raise concerns analogous to those addressed by the DMA.

At the same time, the discussion extended beyond competition concerns. Questions of sovereignty, resilience, and exposure to external legal frameworks were raised, reflecting the growing perception of cloud as critical infrastructure within the European digital economy.

Finally, the timing of regulatory intervention emerged as a central issue. While some participants stressed the importance of early action, others cautioned against regulating markets that remain in rapid evolution. As one participant observed, there is a risk of "building the house from the roof"—that is, designating gatekeepers before establishing whether the DMA is the appropriate framework for cloud at all.

This report does not seek to resolve these tensions. Rather, it aims to structure them through three alternative scenarios for the application of the DMA to cloud markets: that the framework can capture cloud within its current structure; that it does not fit the sector's characteristics; or that it may require adaptation.

CLOUD AS CRITICAL INFRASTRUCTURE: MARKET REALITY

01

2. CLOUD AS CRITICAL INFRASTRUCTURE: MARKET REALITY

> Cloud computing has evolved into a core layer of digital infrastructure. In **2025**, 52.7 percent of EU enterprises used paid cloud services, an increase of over seven percentage points compared with **2023**. Among enterprises using paid cloud services, 77.5 percent were classified by Eurostat as highly dependent on cloud, meaning they had purchased at least one sophisticated service such as database hosting, security software, or computing platforms for application development.[4] The EU's Digital Decade policy program reflects this growing centrality by setting a target of 75 percent enterprise cloud adoption by 2030.[5]

This dependency is reinforced by the role of cloud computing as the core infrastructure for artificial intelligence. Training and deploying AI models require the scale of computing resources that only cloud infrastructure can efficiently provide. As AI becomes more deeply embedded in economic activity, the strategic importance of the underlying cloud layer intensifies correspondingly. Cloud and AI are not merely adjacent markets; they are structurally interdependent, each amplifying the centrality of the other.[6]

The relationship runs in both directions. AI workloads are among the fastest-growing sources of cloud demand, already accounting for a significant share of the market's recent growth. At the same time, the three leading cloud providers—AWS, Microsoft Azure, and Google Cloud—are also among the dominant providers of AI infrastructure, including accelerated compute, model-as-a-service platforms, and integrated development environments. The UK Competition and Markets Authority (CMA) July 2025 final decision on cloud infrastructure services found that while AI has not yet materially altered competitive dynamics in cloud, AI capabilities are likely to become more important to customers over time and could impact competition in cloud services to a greater degree in the future.[7] This convergence means that regulatory choices about cloud increasingly shape the competitive conditions for AI—and vice versa. The question of whether and how the DMA applies to cloud cannot be fully assessed without accounting for this deepening interdependence.

At the same time, supply is highly concentrated. As of the fourth quarter of 2025, AWS held approximately 29 percent of the global cloud infrastructure market, Microsoft Azure approximately 20 percent, and Google Cloud Platform approximately 13 percent.[8] In Europe, the three hyperscalers account for an estimated 65 to 70 percent of cloud infrastructure revenues.[9] The combined share of European cloud providers has declined from approximately 26 percent in 2017 to around 13 to 15 percent today.[10] This concentration reflects deep structural features—high fixed costs for data center construction, pronounced economies of scale and scope, and ecosystem integration—that systematically favor incumbents and create durable barriers to entry and expansion.[11]

Barriers to contestability are well documented across multiple jurisdictions. Competition authorities and market studies have identified three main categories of barriers.[12] The first is contractual: egress fees charged for transferring data out of a cloud environment, committed spend agreements that lock customers into minimum expenditure levels, and cloud credits that disproportionately steer early-stage companies toward hyperscalers.[13] The second is technical: API incompatibility across providers, limited interoperability

between cloud environments, data portability constraints, and the need for costly application re-architecture when switching.[14] The third is strategic: software licensing restrictions that make it more expensive to use certain products on competing cloud platforms, bundling of cloud services with adjacent offerings, and ecosystem leverage.[15]

These barriers interact and reinforce one another. A customer that has invested in optimizing workloads for a particular provider's proprietary tools, trained staff on that provider's technology, and entered into multi-year committed spend agreements faces cumulative switching costs that may be prohibitive in practice. As the CMA observed in its July 2025 final decision, switching between public cloud providers is extremely rare, and the combination of low switching rates and sustained profitability among leading providers is consistent with the presence of significant barriers to switching.[16]

A key distinction emerges between transactional frictions and structural dependency. While some barriers can be addressed through targeted measures such as portability rules or limits on switching charges, others are embedded in organizational processes, technical architectures, and ecosystem integration. This distinction is critical for regulatory analysis: transactional frictions fall primarily within the scope of the Data Act, while structural dependency raises questions that may require different regulatory instruments.[17]

Software licensing practices were also discussed at the working breakfast as a potential source of competitive concern. Licensing practices—including restrictions on "bring your own license" rights when deployed on rival cloud platforms—may affect the conditions under which software products are used across competing infrastructures, reinforcing switching costs and ecosystem integration.[18]

This is significant for the broader regulatory debate as it identifies a mechanism of market power—leveraging dominance in adjacent software markets into cloud infrastructure—that falls between the scope of existing regulatory instruments. The DMA's obligations, even if triggered by designation, do not specifically address cross-market licensing practices in the cloud context. The Data Act targets switching charges and interoperability but does not extend to the licensing terms that condition how software products may be used across competing infrastructure.[19] Software licensing may be understood as a potential post-regulatory adaptation: as traditional lock-in practices such as egress fees are addressed by regulatory interventions, attention has shifted toward more subtle mechanisms that may raise comparable concerns, including licensing terms that affect the portability and use of software across cloud environments.[20]

These issues remain contested. Some stakeholders have argued that competition in cloud does not turn on the pricing of legacy software, that open-source alternatives dominate key segments of the public cloud, and that component-level analyses may not fully reflect how cloud services are purchased in practice, which typically involves bundled offerings.[21] The analytical question—whether licensing practices constitute a structural barrier or a legitimate exercise of intellectual property rights—therefore remains open.

Taken together, these dynamics suggest that cloud markets exhibit forms of power that are *infrastructural rather than intermediary in nature*, arising not from direct intermediation between user groups, but from control over critical infrastructure and the ecosystems built upon it.

52.7 % of EU enterprises used paid cloud services in 2025, an increase of over seven percentage points compared with 2023.

THE DMA AND CLOUD: A STRUCTURAL MISMATCH

03

3. THE DMA AND CLOUD: A STRUCTURAL MISMATCH

> The difficulty in applying the DMA to cloud computing reflects a structural misalignment between the regulation's conceptual framework and the economic structure of cloud markets.

The DMA conceptualizes gatekeepers as intermediaries between business users and end users. This model presupposes the existence of multi-sided platforms. Cloud computing services, particularly at IaaS and PaaS levels, operate differently. They form a *vertical pipeline*, where providers supply infrastructure to businesses, which then serve end users.[22] This creates a "gateway problem": cloud providers do not directly intermediate access to end users. Instead, their influence is exercised indirectly through downstream services.[23]

This has direct implications for the DMA's quantitative designation thresholds. The Annex to the DMA approaches the notion of active end users through a methodology based on "unique users" who engage with the service within a given period, in return for remuneration. In the context of cloud computing services, this approach effectively captures the direct customer base of the provider. At the IaaS and PaaS levels, these users are primarily enterprise customers rather than mass consumers, and their number remains well below the 45 million monthly active end-user threshold. This is not simply an empirical gap that will close as cloud adoption grows, but reflects the structural way in which cloud services are consumed.[24]

The DMA provides an alternative route through Article 3(8), which allows qualitative designation when the quantitative thresholds are not met. This is the route now being pursued in the Commission's investigations into AWS and Azure.[25] However, the qualitative route does not resolve the fundamental conceptual difficulty. Of the three qualitative criteria—significant impact on the internal market, important gateway for business users to reach end users, and entrenched and durable position—the first and third are satisfied by the leading hyperscalers. The critical legal obstacle is the second: the "important gateway" requirement. The qualitative factors enumerated in Article 3(8)—network effects, scale and scope economies, data advantages, user lock-in, conglomerate structure, and vertical integration—are indicators of the importance of an *existing* gateway, explaining why a platform that already functions as one is likely to entrench its position. But they cannot construct a gateway function where intermediation between business users and end users is structurally absent or attenuated. A qualitative assessment that relies solely on economic characteristics without conceptually establishing the gateway relationship would conflate market power with the specific regulatory concept of gatekeeping that the DMA is designed to address.[26]

Two possible pathways for qualitative designation have been proposed in the literature. The first focuses on cloud marketplaces. All three hyperscalers operate marketplace services through which customers can discover and purchase not only the hyperscaler's own services but also PaaS and SaaS products from independent software vendors (ISVs). In this configuration, hyperscalers introduce genuine two-sided platform dynamics, intermediating between ISV business users on the supply side and enterprise customers on the demand side. The second pathway relies on what has been termed "indirect ecosystem capture"—the notion that hyperscalers exercise gatekeeping power through the vertical integration of infrastructure, platform services, and downstream applications within a single ecosystem, generating dependencies that are structurally more severe than

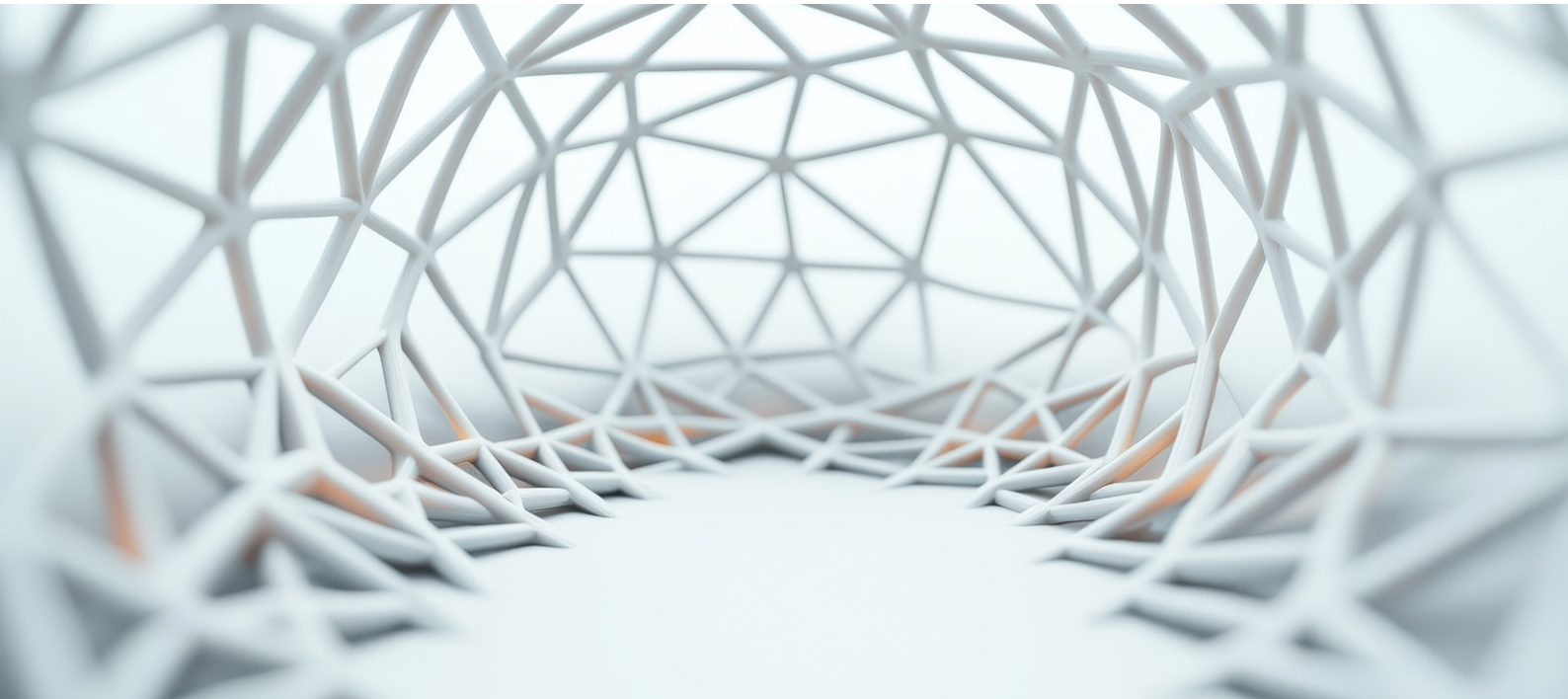
those of a pure intermediation platform.[27] Both pathways are analytically coherent, but may end up stretching the DMA's conceptual framework beyond its original design parameters.

Even if designation were to proceed, a further challenge remains: the DMA's obligations are not well calibrated for cloud services. While the Commission may rely on delegated acts under Articles 12 and 49 to introduce limited adjustments, the primary mechanism for addressing structural gaps in the framework lies in the market investigation process under Article 19, which allows for a broader reassessment of practices and remedies. A careful mapping reveals that the provisions applicable to cloud are significantly narrower than those applicable to other core platform services such as search engines, app stores, or social networks.[28] The most notable gap is the absence of a cloud-to-cloud interoperability mandate. Article 7 establishes a strong interoperability regime, but it applies only to number-independent interpersonal communications services—that is, messaging. Cloud services are excluded from this regime, despite interoperability being central to the contestability concerns identified in cloud markets.[29] Other applicable obligations—including restrictions on combining personal data without consent (Article 5(2)), prohibitions on tying (Articles 5(7) and 5(8)), and data portability requirements (Articles 6(9) and 6(10))—were drafted with consumer-facing platform services in mind and do not address the specific competition concerns identified in cloud markets.[30]

This obligation gap has been acknowledged by the Commission itself. The third market investigation, discussed above, explicitly examines whether the DMA's obligations need to be updated for cloud.[31] This creates a structural tension: the Commission is simultaneously pursuing designation under a framework whose suitability for cloud markets remains under assessment.[32]

A further technical but consequential issue relates to definitional inconsistency. The DMA defines cloud computing services by reference to Directive 2016/1148 (the original NIS Directive), which has since been replaced by Directive 2022/2555 (NIS2), providing a more detailed definition encompassing distributed architectures and additional service models.[33] Separately, the Data Act does not use the term "cloud computing services" at all, subsuming cloud within the broader concept of "data processing services."[34] This means that key instruments addressing cloud at the EU level do not share the same definitional language, reflecting the broader fragmentation that characterizes the EU's approach to cloud governance.

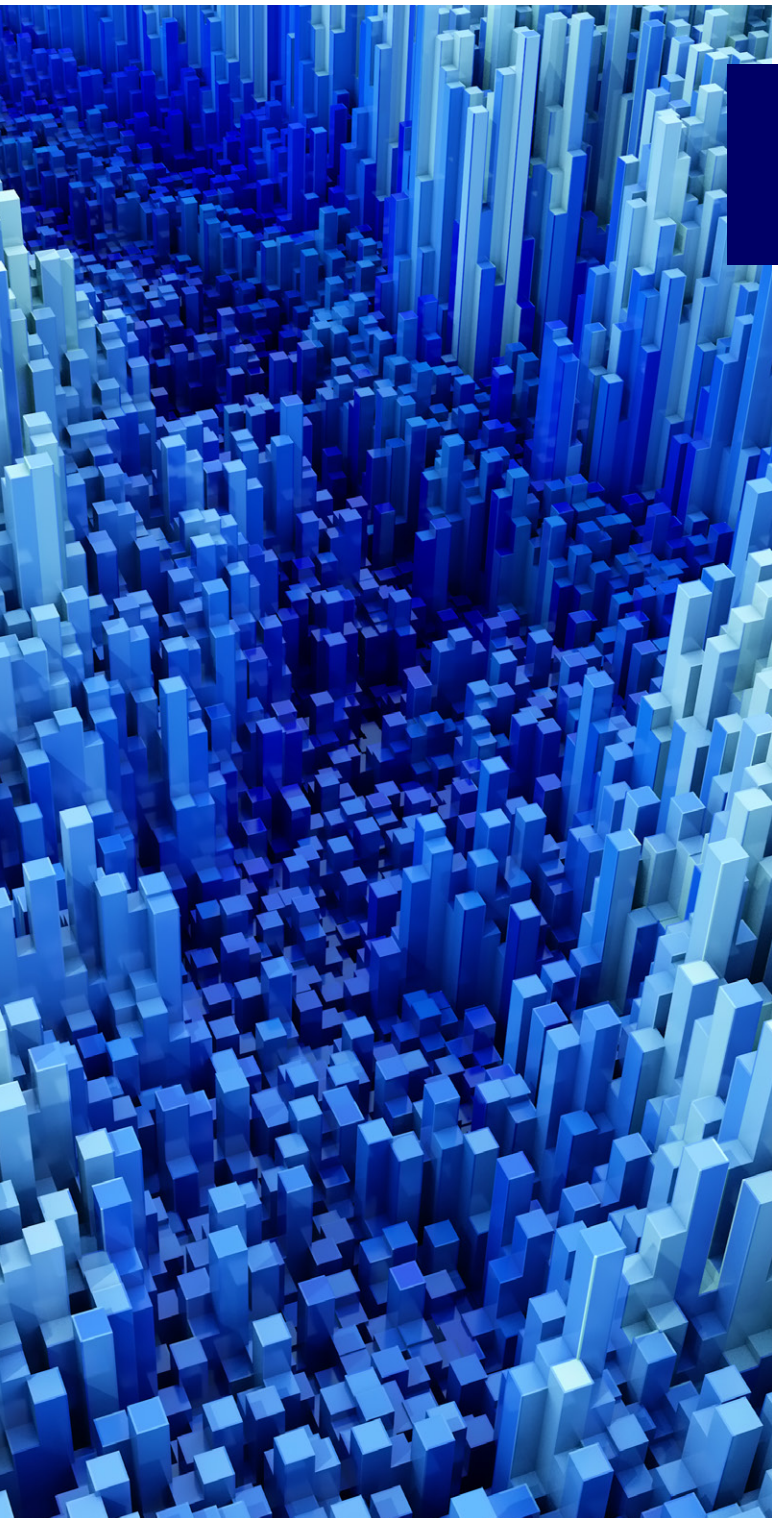
The issue, therefore, is not simply whether the DMA applies to cloud, but how its core concepts should be interpreted in the context of infrastructure-driven markets. More fundamentally, it raises the question of whether a regulatory framework designed around intermediation can adequately capture forms of market power that are embedded in the control of digital infrastructure.



COMPETING INTERPRETATIONS: THREE SCENARIOS FOR CLOUD MARKETS

04

4. COMPETING INTERPRETATIONS: THREE SCENARIOS FOR CLOUD MARKETS



4.1 THE DMA CAN CAPTURE CLOUD

Interpretation:
The absence of designation reflects an enforcement gap, not a limitation of the framework.

Under this perspective, cloud services fall within the DMA's scope, and the lack of intervention reflects a delay in applying existing tools rather than a limitation of the framework itself. Proponents emphasize concentration, switching barriers, and the strategic importance of cloud infrastructure as grounds for qualitative designation. The cloud marketplace and integrated intermediation frameworks discussed above offer possible pathways for establishing the gateway function under Article 3(8).[35]

This position has been advanced with particular force by civil society organizations and members of the European Parliament, who argue that further delay in designating cloud providers risks undermining both the effectiveness and the credibility of the DMA. From this perspective, it was never the intention of the EU legislator to exclude hyperscalers from the scope of the regulation simply because the forms of network effects observed in other digital services are less pronounced in cloud markets. Rather, the gatekeeping power of hyperscalers is understood to derive from economies of scale, lock-in effects, vertical integration, and data-driven advantages—factors that the DMA was designed to address.[36] The Commission's decision to open qualitative designation investigations lends institutional weight to this interpretation. Some participants in the working breakfast, as well as contributions to the broader policy debate, raised the question of whether, in the event of designation of certain hyperscalers, similar considerations could arise for other major providers.

4.2 THE DMA DOES NOT FIT CLOUD

Interpretation:
The DMA's design does not map onto infrastructure markets where intermediation is indirect or absent.

The gatekeeper model—based on intermediation—does not map onto infrastructure markets where intermediation is indirect or absent. As a result, both quantitative thresholds and qualitative criteria may fail to capture economically relevant forms of power. In its most far-reaching form, this position suggests that cloud computing services may not belong within the DMA's conceptual framework at all. Under this view, the inclusion of cloud among core platform services could be reconsidered in the context of the Article 53 review—a step that would require acknowledging a potential misalignment in the original legislative design.[37]

While analytically coherent, this position faces considerable obstacles. Removing cloud from the list of core platform services would require the Commission to concede that the original legislative choice was, at least in part, a misjudgment—a step with obvious political costs. It would also leave the structural competition concerns identified by multiple competition authorities without a dedicated asymmetric instrument.

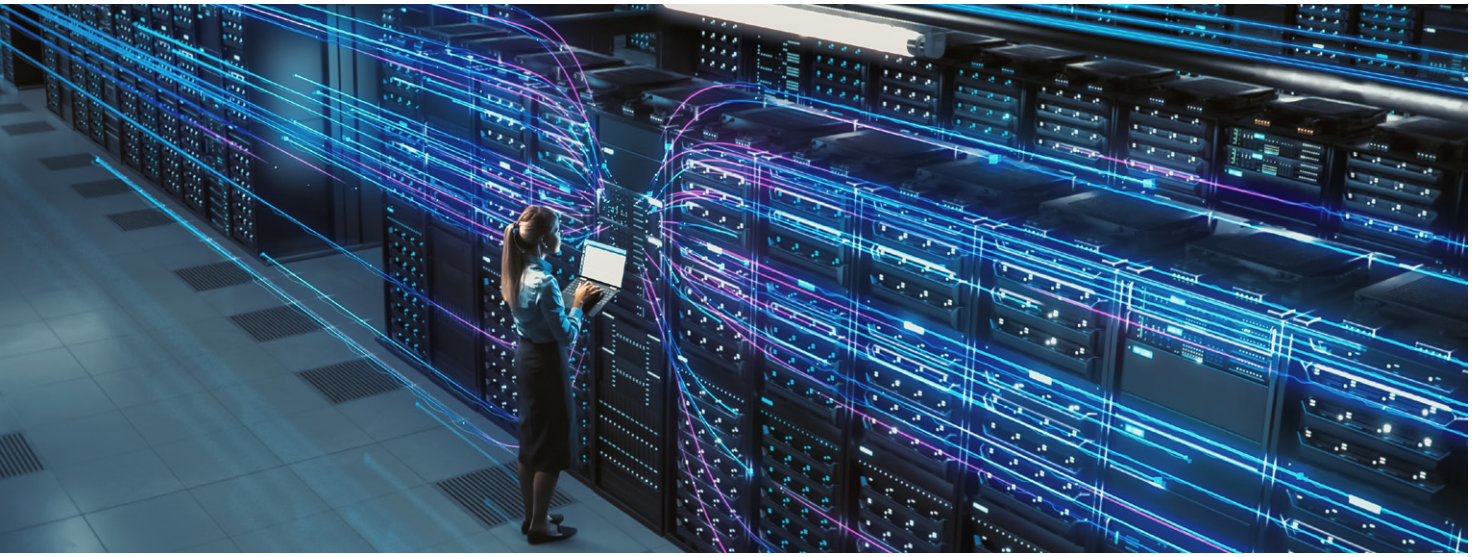
4.3 THE DMA CAN ADAPT

Interpretation:
The framework can evolve through qualitative designation, delegated acts, or reinterpretation of core concepts.

This position recognizes that cloud services may not fit the traditional platform model, but argues that gatekeeping power can nonetheless emerge through ecosystem integration, vertical leverage, and structural dependency. Under this approach, the DMA may be adapted through interpretation, qualitative designation, or adjustments to its operational mechanisms.[38]

These scenarios are not mutually exclusive. Rather, they represent different ways of understanding the problem: as one of enforcement, of legal design, or of regulatory adaptation.

The discussion at the working breakfast reflected all three positions. Some participants stressed the need for timely intervention to prevent further entrenchment. Others highlighted the conceptual difficulties of applying the DMA to business-to-business infrastructure markets. A third group highlighted the possibility of incremental adaptation through existing mechanisms. Across these perspectives, a common concern emerges: whether the conceptual apparatus of the DMA is capable of capturing forms of power rooted in infrastructure rather than intermediation.



TIMING, INVESTIGATIONS, AND REGULATORY UNCERTAINTY

05

5. TIMING, INVESTIGATIONS, AND REGULATORY UNCERTAINTY

The question of how the DMA applies to cloud markets is not only conceptual, but also temporal, particularly in terms of timing and sequencing. As noted, the Commission's November 2025 investigations pursue a dual-track approach—simultaneously testing both capture (whether AWS and Azure qualify as gatekeepers) and fit (whether the DMA's obligations are adequate for cloud).[39] This is analytically significant: the Commission is not merely enforcing an existing framework, but evaluating its suitability in real time. Notably, the investigations refer to practices that may limit "competitiveness and fairness," a formulation that departs from the DMA's own language of "fairness and contestability" and suggests a broader understanding of cloud as both market and infrastructure.

The discussion at the working breakfast revealed divergent views on the timing of intervention. Some participants emphasized the risks of delay in markets characterized by economies of scale, network effects, and cumulative lock-in. The OECD has observed that, in such contexts, timely intervention may be necessary to preserve effective competition before market structures become further entrenched.[40] The CMA's finding that full switching between cloud providers is "extremely rare" reinforces this concern.[41]

Cloud markets are evolving rapidly: new entrants are emerging, generative AI is reshaping demand patterns, and local solutions may gradually reduce dependency. In this context, several participants argued that designation should not precede a clear assessment of whether the DMA is the appropriate regulatory framework. Voluntary codes of conduct were suggested as a potential transitional mechanism, capable of addressing certain concerns while preserving flexibility. Others emphasized the importance of allowing existing instruments—particularly the Data Act and competition law—to produce effects before introducing additional layers of regulation.

The experience of the SWIPO codes of conduct provides a relevant reference point. Developed under the Free Flow of Non-Personal Data Regulation, these voluntary mechanisms had limited uptake and impact, ultimately contributing to the adoption of binding rules under the Data Act.[42] This experience suggests that voluntary approaches may play a useful transitional role, but are unlikely to substitute for binding intervention where structural barriers persist.

These considerations reinforce the importance of a dynamic perspective. The issue is not only whether the DMA applies to cloud, but when and under what conditions its application would be most effective. The Commission's first review of the DMA, published in April 2026, reinforces this dynamic. While concluding that the DMA remains fit for purpose overall, the review explicitly identifies cloud computing services as an area requiring further assessment, reflecting the fact that the application of the framework to infrastructure-driven markets remains unsettled.

The issue is not only whether the DMA applies to cloud, but when and under what conditions its application would be most effective. The Commission's first review of the DMA, published in April 2026, reinforces this dynamic.

THE REGULATORY LANDSCAPE: COMPLEMENTARITY AND FRAGMENTATION

06

6. THE REGULATORY LANDSCAPE: COMPLEMENTARITY AND FRAGMENTATION

> Cloud markets cannot be understood through the DMA in isolation. They are subject to a layered regulatory framework that addresses different dimensions of the same phenomenon.

The Data Act plays a significant role. Unlike the DMA, it applies symmetrically to all providers of data processing services and focuses on reducing switching barriers through portability, interoperability, and limits on switching charges.[43] This distinction is central to the regulatory analysis. The Data Act addresses *transactional frictions*, while the DMA is designed to address *structural market power*.[44]

The Data Act's provisions on switching (Chapter VI) establish binding rules that require providers to support customer switching, limit the transition period to 30 days, and mandate the elimination of switching charges. Between January 2024 and January 2027, providers may charge only the direct costs of switching; from January 2027, such charges must be eliminated entirely.[45] The Data Act also requires providers of PaaS and SaaS services to make open interfaces publicly available and to ensure compatibility with common specifications or harmonized standards for interoperability (Chapter VIII).[46]

There are early signs that the Data Act is already producing market effects. In response to the legislation, Microsoft, AWS, and Google have introduced free switching programs globally—including for UK customers not directly subject to the regulation.[47] While the CMA cautioned that uptake has been low and the programs' voluntary nature makes them revocable, they represent a concrete shift in provider behavior traceable to regulatory pressure.[48] The interoperability provisions depend on the development of technical standards.

In July 2025, the European Commission issued a standardization request to CEN and CENELEC, which agreed to develop standards supporting cloud provider switching and interoperability—though the timeline for completion remains uncertain.[49]

The question of sequencing—whether to allow the Data Act to produce effects before layering additional obligations through the DMA—emerged as a central theme of the discussion. The Data Act addresses the most immediate and tangible barriers, and its symmetric approach avoids the designation bottleneck that has paralyzed the DMA's application to cloud. At the same time, the Data Act does not address market power directly. Without the DMA or equivalent instruments, structural competition concerns may persist even as transactional barriers are reduced.[50]

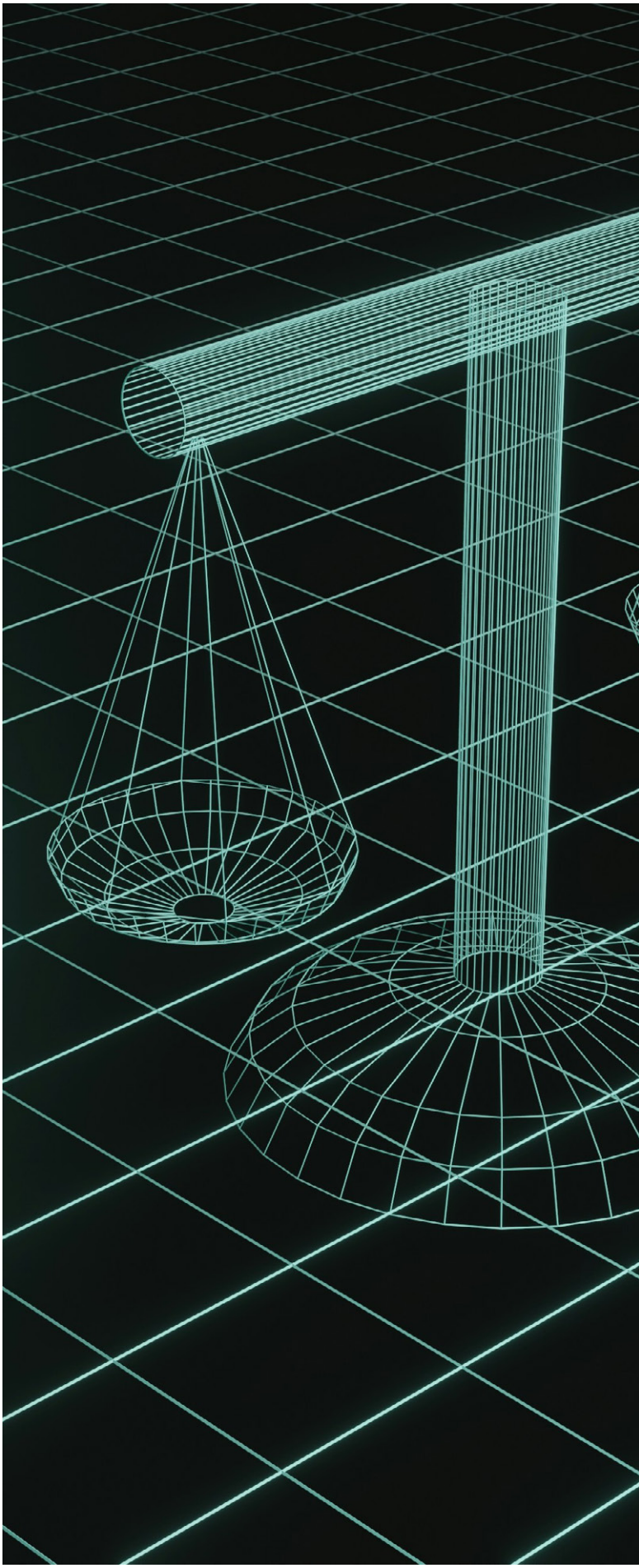
Additional frameworks address resilience and security. NIS2 establishes baseline cybersecurity obligations for digital infrastructure providers, including cloud services, while DORA introduces sector-specific oversight of critical ICT providers in the financial sector through the European Supervisory Authorities.[51] These instruments address dimensions of cloud governance that neither the DMA nor the Data Act are designed to capture: the systemic risk arising from concentration of critical infrastructure in a small number of providers, the operational resilience of services on which entire economic sectors depend, and the security implications of dependency on non-EU infrastructure.

The coexistence of these frameworks creates complementarities, but also coordination challenges. Overlaps in scope—particularly between NIS2 and DORA on incident reporting and audit requirements—differences in implementation across Member States, and reliance on future standards create uncertainty for

market participants.[52] The Digital Omnibus proposal, published by the Commission in November 2025, aims to streamline overlaps across the EU digital regulatory framework, notably by reducing duplicative reporting requirements and clarifying the interplay between instruments.[53] But fundamental challenges persist, particularly as these instruments are enforced at different levels—the DMA centrally by the Commission, the Data Act and NIS2 by national authorities, and DORA by the European Supervisory Authorities.

In the absence of DMA designation, regulatory intervention relies primarily on symmetric instruments and sectoral frameworks. The result is a regulatory architecture that is both layered and incomplete, addressing multiple dimensions of cloud governance without providing a fully coherent framework.

> The coexistence of these frameworks creates complementarities, but also coordination challenges.



SOVEREIGNTY, SECURITY, AND STRATEGIC AUTONOMY

07

7. SOVEREIGNTY, SECURITY, AND STRATEGIC AUTONOMY

Cloud computing is now widely treated not only as a market, but as strategic infrastructure. EU institutions have linked cloud governance to broader objectives such as innovation, resilience, and strategic autonomy.[54] The dominance of a small number of non-EU providers raises concerns about dependency and exposure to external legal frameworks that extend beyond competition.

The working breakfast confirmed the centrality of these concerns. Participants from government emphasized that security considerations now sit alongside competition as a core concern, particularly in the current geopolitical context. Particular attention was given to regulatory exposure risks arising from the US CLOUD Act—the Clarifying Lawful Overseas Use of Data Act of 2018—which allows US law enforcement authorities, subject to applicable legal process, to compel providers subject to US jurisdiction to produce data within their possession, custody, or control, regardless of where that data is stored or the nationality of the data subject.[55]

Industry perspectives offered a counterpoint. It was argued that mechanisms exist to mitigate sovereignty risks, including contractual commitments allowing providers to challenge government access requests, potentially up to the level of the US Supreme Court. On this view, the CLOUD Act applies only in the context of criminal investigations supported by probable cause, and data remains under the control of customers rather than providers. It was further argued that, at least in the experience of the provider represented in the discussion, no requests under the Act have resulted in the disclosure of European customer data, and that concerns about exposure may therefore be overstated.[56]

However, these assurances face structural limitations. The legal architecture of the CLOUD Act applies to any company subject to US jurisdiction—including US-headquartered firms and their European subsidiaries. Only cloud service providers with a European parent company that has no US nexus can fully avoid the jurisdictional reach of the Act.[57] This concern has been identified not only in the policy debate but also by competition authorities: the Dutch Competition Authority (ACM) 2022 market study on cloud services flagged the risks associated with the storage and processing of data by providers subject to non-EU legal frameworks as a factor relevant to the assessment of cloud market functioning.[58] This suggests that contractual commitments, however robust, cannot entirely eliminate the extraterritorial risk as long as the corporate structure remains subject to US law.

It is also important to recognize that extraterritorial data access is not uniquely a US phenomenon. Spain's Ley de Enjuiciamiento Criminal, for example, allows judges to request data stored outside Spain. European companies can themselves fall under the CLOUD Act if they have a US nexus. The challenge of cross-jurisdictional data governance is structural rather than unilateral, and responses should be calibrated accordingly.

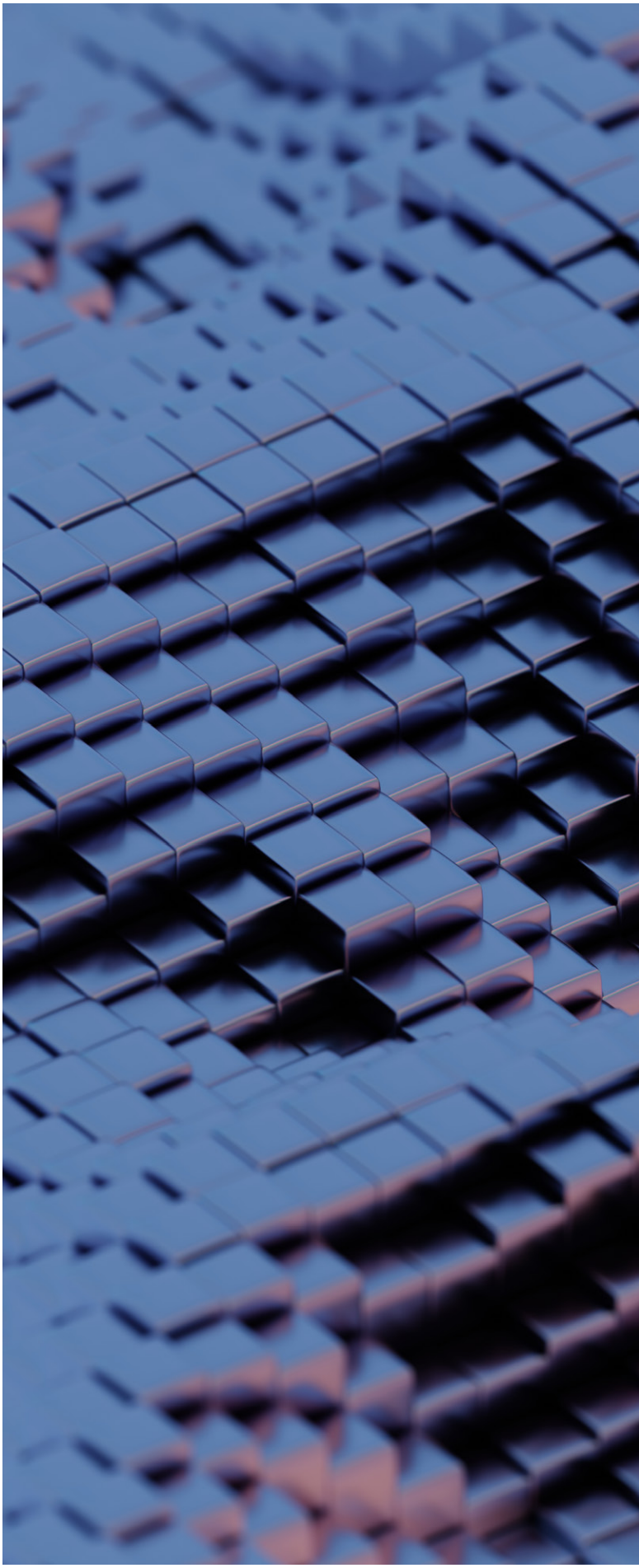
Participants from government emphasized that security considerations now sit alongside competition as a core concern, particularly in the current geopolitical context.

The sovereignty dimension is also reflected in the European Cybersecurity Certification Scheme for Cloud Services. An updated draft issued by ENISA in 2023 proposed a highest assurance level including requirements aimed at limiting exposure to non-EU legal frameworks, notably through conditions relating to control, ownership, and jurisdiction.[59] While these requirements are politically understandable, they introduce geopolitical considerations that should be clearly distinguished from economic and technical assessments.[60]

The proper boundary between competition regulation and industrial policy also requires attention. The risk of zero-sum thinking—the assumption that making US companies marginally worse off will automatically create opportunities for European firms—was highlighted during the working breakfast as misguided, given the vast differences in investment levels and capabilities between the US and the EU. The objective should be a genuine level playing field rather than the promotion of specific market outcomes.

The experience of GAIA-X illustrates the limitations of a direct investment approach. Despite significant resources, the initiative has produced limited practical results and evolved into what has been described as a bureaucratic standard-setting exercise rather than a competitive market participant.[61] By contrast, public procurement has proven more effective as a tool for building cloud diversity and reducing dependency—a finding with important implications for policy design.

The strategic dimension of cloud markets therefore reinforces—rather than replaces—the analytical questions identified in this report. It highlights the broader implications of market structure and dependency, while underscoring the importance of maintaining conceptual clarity between competition regulation and industrial policy. In this context, sovereignty and resilience objectives are likely to be most effectively pursued through dedicated instruments—including procurement policy, cybersecurity frameworks, and strategic investment—rather than through the extension of regulatory tools beyond their original design.



POLICY DIRECTIONS

08

8. POLICY DIRECTIONS

The analysis suggests that cloud markets cannot be effectively addressed through a single regulatory instrument. Rather than pointing to a single solution, it suggests a set of policy directions that reflect different ways of approaching the relationship between the DMA and cloud computing.

Sequencing regulatory intervention.
Several elements of the current framework—particularly the Data Act—are specifically designed to address switching barriers and interoperability constraints, which have been identified as some of the most immediate obstacles to contestability in cloud markets. The phased implementation of the Data Act's provisions, extending through 2027, suggests that its impact is still unfolding. This does not diminish the distinct role of the DMA, which is designed to address structural market power through an asymmetric framework. Rather, it highlights the importance of sequencing these instruments as coordination between complementary regulatory approaches, not as substitution.

Adapting the DMA's conceptual framework.
If the DMA is to be applied to cloud markets, its conceptual and operational framework is likely to require adjustment. This creates a natural opportunity to reassess the relevance of key concepts, including the definition of business and end users, the scope of interoperability obligations, and the calibration of conduct requirements. Any such adaptation would need to be carefully designed to avoid duplicating the Data Act or introducing obligations that are difficult to operationalize in infrastructure-driven contexts.

Addressing areas not fully captured by the current framework.
One such area, highlighted in both the literature and the discussion, relates to software licensing practices as a mechanism of lock-in. While aspects of these concerns may be addressed through competition law enforcement,[62] they are not directly captured by the design of the DMA or the Data Act. This suggests the need for a more targeted and coordinated use of existing instruments to address cross-market dynamics in cloud environments.

Coordinating the regulatory ecosystem.
The coexistence of the DMA, the Data Act, NIS2, DORA, and related frameworks creates both complementarities and coordination challenges. Ensuring coherence across these instruments—particularly with respect to reporting requirements, oversight mechanisms, and enforcement practices—will be essential to avoid fragmentation and to provide clarity for market participants.

Leveraging procurement and flexible mechanisms.
Governments retain major influence over cloud markets through procurement, standard-setting, and strategic investment. Public procurement in particular emerges as a powerful tool for shaping market outcomes—encouraging multi-cloud architectures, promoting interoperability, and supporting provider diversity. Evidence discussed during the working breakfast suggests that procurement has, in some cases, been more effective than direct investment initiatives in fostering market diversification. Voluntary mechanisms may serve as useful transitional tools, though as earlier experience has shown, they are unlikely to address structural barriers in the absence of binding obligations.

Preserving the distinction between competition regulation and industrial policy.
While concerns relating to sovereignty and resilience are legitimate and increasingly prominent, the DMA is not designed to promote specific market outcomes or favor particular providers. Its role is to ensure fairness and contestability. Other objectives—including the development of domestic capacity and the reduction of strategic dependency—are more appropriately pursued through targeted policy instruments, such as procurement strategies, certification frameworks, and investment programs.

For market participants, these developments carry operational implications: as regulatory expectations evolve, proactive investment in multi-cloud strategies, contractual flexibility, and interoperability capabilities may become a key component of both compliance and risk management.

9. CONCLUSION

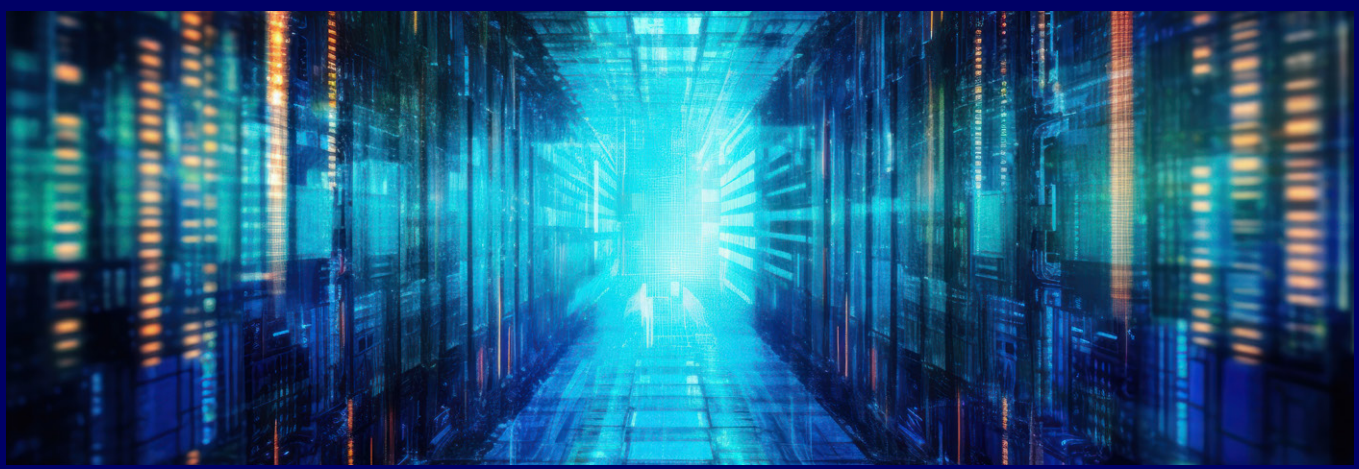
The application of the DMA to cloud computing cannot be resolved through a simple extension of existing regulatory categories. While cloud services are formally included within the scope of the regulation, their effective capture remains uncertain.

This uncertainty reflects a broader tension between the DMA's platform-based logic and the infrastructure-driven nature of cloud markets. In this context, market power arises less from intermediation than from vertical integration, ecosystem control, and structural dependency. The absence of designation should therefore not be interpreted solely as an enforcement gap, but also as an indication of the limits of applying a platform-based framework to infrastructure markets.

At the same time, persistent concerns relating to concentration, switching barriers, and dependency suggest that the underlying issues addressed by the DMA—fairness and contestability—remain highly relevant in the cloud context. The European Commission's ongoing investigations reinforce this duality, confirming that the challenge is not only whether the DMA applies, but whether it is fit for purpose.

The three scenarios outlined in this report—capture, mismatch, and adaptation—do not represent mutually exclusive outcomes, but alternative ways of interpreting the relationship between the DMA and cloud markets. These scenarios reflect different conceptions of how market power operates in cloud environments and, correspondingly, different views on the appropriate role of regulation.

The Article 53 review, published in April 2026, together with the outcome of the Commission's ongoing market investigations, provides an important test of the EU's ability to address this challenge. While the review confirms that the DMA remains fit for purpose, it also underscores that its application to cloud computing services remains an open question. The contribution of this report—and of the discussion that informed it—is to clarify the terms of that challenge and to map the directions through which it may be addressed over time. But the underlying question reaches beyond cloud, and beyond the DMA: as the boundary between platforms and infrastructure becomes increasingly blurred, digital regulation must confront whether frameworks designed to govern one type of market organization can adequately capture the dynamics of another.



ENDNOTES

1 Alex Roche (Senior Associate Director, Center for Governance of Change at IE University), Almudena Martín Castro (Advisory Officer, Directorate General for Strategic Projects and Sectoral Policies, Office of Economic Affairs and G20, Presidency of the Government of Spain), Antonio Estella (Jean Monnet Chair "ad personam" of Law of European Economic Governance, University Carlos III of Madrid), Carlos Luca de Tena (Executive Director, Center for Governance of Change at IE University), Carmen Delibes (Deputy Director General for Better Regulation, Business Support and Competition, Directorate General for Economic Policy, Ministry of Economy, Trade and Business), Ferran Casadevall (Deputy Director, Information Society, National Commission on Markets and Competition), Francisco José Casarrubios (Responsible for AI and Cloud Regulation, Directorate General for AI, Secretariat of State for Digitalization and AI, Ministry for Digital Transformation and the Civil Service), Francisco Pérez Bes (Deputy President, Spanish Data Protection Agency), Gabriel López Serrano (Director of Institutional Relations and Regulatory Affairs, Microsoft), Irene Blázquez Navarro (Director, Center for Governance of Change at IE University), Inés Pérez Durántez (Deputy Director General for International Trade in Services and Digital Trade, Secretariat of State for Trade, Ministry of Economy, Trade and Business), Jeff Bullwinkel (Vice President and Deputy General Counsel, Corporate External & Legal Affairs, Microsoft EMEA), Laura Zoboli (Professor of Competition Law and Tech Regulation, IE University), Lazar Radic (Professor of Digital Competition Regulation, IE University), Natalia Ortiz (Junior Manager, Center for the Governance of Change at IE University), Oriol Armengol (Partner, Competition and EU Law, Garrigues), Patricia Vidal (Partner, Competition and EU Law, Uría Menéndez), Pedro Hinojo (Deputy Director of Research and Analysis, Competition Promotion Department, National Commission on Markets and Competition), and Tomás Arranz (Partner, Competition and EU Law, Uría Menéndez).

2 European Commission, 'Commission launches market investigations on cloud computing services under the Digital Markets Act' (Press Release, 18 November 2025, IP/25/2717).

3 European Commission, Report on the Review of Regulation (EU) 2022/1925 (Digital Markets Act) COM(2026) 178 final, accompanied by Commission Staff Working Document SWD(2026) 123 final.

4 Eurostat, 'Cloud computing—statistics on the use by enterprises' (January 2026).

5 European Commission, 'Digital Decade—Policy programme' (2021).

6 Autorité de la concurrence, Opinion 24-A-05 of 28 June 2024 on the Competitive Functioning of the Generative Artificial Intelligence Sector.

7 Competition and Markets Authority (CMA), *Cloud Infrastructure Services: Final Decision Report* (31 July 2025) paras 4.105–4.144.

8 Synergy Research Group (Q4 2025).

9 Judith Arnal, *Towards Competitive Cloud Ecosystems: Strategic Responses for Europe's Digital Future* (Center for the Governance of Change, July 2025) 5–6.

10 Tech Policy Press, 'Cloud Services Face Scrutiny Under the Digital Markets Act' (18 November 2025), citing Francesco Bonfiglio, former CEO of Gaia-X.

11 Antonio Manganelli, *Gatekeepers in the Cloud: Integrated Intermediation, Indirect Ecosystem Capture, and the Case for Cloud Neutrality* (Konrad-Adenauer-Stiftung, 2026) 8–9; CERRE, *Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies* (2024) 68–72.

12 These categories are drawn from the convergent findings of the ACM (Autoriteit Consument & Markt, Market Study Cloud Services (2022)), CMA (n 7), Autorité de la concurrence (n 6), OECD, *Competition in the Provision of Cloud Computing Services*, OECD Roundtables on Competition Policy Papers No 323 (2025) 18–26; and CERRE (n 11 above).

13 OVHcloud, *Response to the CMA Cloud Services Market Investigation's Provisional Decision Report* (21 February 2025) paras 9–14.

14 CMA (n 7) ch 6; CERRE (n 11) 73–92.

15 Frédéric Jenny, *Cloud Infrastructure Services: An Analysis of Potentially Anti-Competitive Practices* (CISPE, October 2021); CMA (n 7) ch 7.

16 CMA (n 7) para 3.457.

17 CERRE (n 11) 80–82.

18 CMA (n 7) paras 6.539–6.543.

19 Kalpana Tyagi, 'Can Europe's Digital Markets Act and Data Act Rein in Cloud Hyperscalers?' (Tech Policy Press, 3 February 2026).

20 Arnal (n 9) 19–20; see also Jenny (n 15) on earlier forms of leveraging.

ENDNOTES

21 Microsoft, *Response to the CMA Provisional Decision Report—Cloud Services Market Investigation* (24 February 2025) paras 36–56.

22 Manganelli (n 11) 13–14.

23 Christophe Carugati, 'Do Cloud Computing Services Fall Under the Digital Markets Act?' (Digital Competition Regime, 26 January 2026) 2–3.

24 Manganelli (n 11) 14–15.

25 Regulation (EU) 2022/1925 (Digital Markets Act), arts 3(8) and 17.

26 Manganelli (n 11) 15–16.

27 Manganelli (n 11) 16–20.

28 Konstantina Bania and Damien Geradin, 'The Regulation of Cloud Computing: Why the European Union Failed to Get It Right' (2024) 33(1) Information & Communications Technology Law 99, 104–108; Tyagi (n 19).

29 DMA, art 7.

30 DMA, arts 5(2)(b)–(d), 5(6)–(8), 6(2), 6(5)–(6), 6(9)–(10), 6(13).

31 Commission Press Release (n 2).

32 Alba Ribera Martínez, *'What the Cloud? The European Commission's Strategy to Counter Challenges on Cloud Computing Services'* (18 November 2025).

33 DMA, art 2(13), referencing Directive (EU) 2016/1148, art 4(19); cf Directive (EU) 2022/2555 (NIS2).

34 Regulation (EU) 2023/2854 (Data Act), art 2(8).

35 ARTICLE 19, *A Review of the Digital Markets Act: Unlocking Contestability and Fairness in Cloud and AI* (2025) 8–10; Open Markets Institute, *Review of the Digital Markets Act—Considerations on Cloud and AI* (2025).

36 ARTICLE 19 (n 35) 9; see also Andreas Schwab, 'The DMA Review: Strengthening Europe's Digital Rulebook' (2025).

37 Bania and Geradin (n 28) 104–108.

38 CERRE (n 11) 101–108.

39 Commission Press Release (n 2).

40 OECD (n 12) 36.

41 CMA (n 7) para 3.457.

42 European Commission, Staff Working Document—Impact Assessment Report accompanying the Data Act proposal, SWD(2022) 34 final; CERRE (n 11) 27.

43 Regulation (EU) 2023/2854 (Data Act), Chapter VI.

44 CERRE (n 11) 101–108; Tyagi (n 19).

45 Data Act, arts 25, 27, 29.

46 Data Act, arts 30, 33–35.

47 CMA (n 7) paras 6.457–6.462.

48 ibid paras 6.482–6.487.

49 CMA (n 7) para 6.256; CEN-CENELEC, 'Data Act: Standardization Request Officially Accepted' (2025).

50 CERRE (n 10) 101–108; Tyagi (n 18).

51 Directive (EU) 2022/2555 (NIS2), Annex I; Regulation (EU) 2022/2554 (DORA), arts 28–44.

52 CERRE (n 11) 53–55.

53 European Commission, Digital Omnibus package (November 2025).

54 Commission Press Release (n 2).

55 18 US Code § 2713; Clarifying Lawful Overseas Use of Data Act (2018).

56 See generally Microsoft, *Response to the CMA Provisional Decision Report* (n 21) paras 57–60, describing the company's European digital commitment and contractual safeguards.

57 MSG for banking AG, *White Paper on Digital Sovereignty in the Cloud* (January 2026) 14–15

58 Autoriteit Consument & Markt (n 12) 60–62.

59 ENISA, EUCS draft (August 2023), Annex I.

60 CERRE (n 11) 62.

61 Arnal (n 9) 26–28.

62 European Commission, Commission accepts commitments offered by Microsoft to address competition concerns related to Teams (Press Release, 12 September 2025), addressing tying, interoperability, and data portability concerns in digital markets.

IE UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

AUTHOR:
Laura Zoboli

RECOMMENDED CITATION:
Zoboli, L., *The DMA Meets the Cloud: Gatekeepers and Beyond*, IE CGC, June 2026

Design: epoqstudio.com
Images: Shutterstock, Unsplash