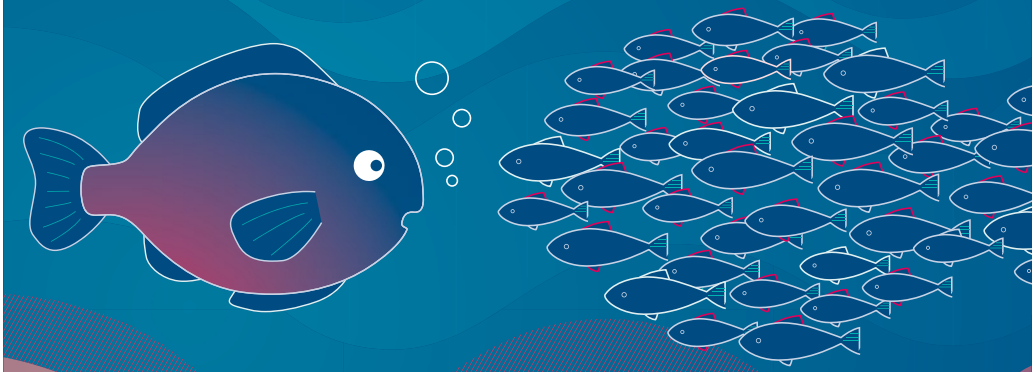
KONRAD ADENAUER STIFTUNG

Gatekeepers in the Cloud

Integrated Intermediation, Indirect Ecosystem Capture, and the Case for Cloud Neutrality

Antonio Manganelli

European Data Summit 2026



kas.de

Gatekeepers in the Cloud

Integrated Intermediation, Indirect Ecosystem Capture, and the Case for Cloud Neutrality

At a Glance

Despite cloud computing services being listed as a core platform service under the Digital Markets Act, no hyperscaler has been designated as a gatekeeper. This paper argues that the persistent failure of designation reflects a structural incompatibility between the DMA's two-sided platform logic and the vertical pipeline architecture of cloud markets – a mismatch that renders both the quantitative thresholds and the qualitative gateway criterion analytically ill-suited to the cloud context. The paper, however, proposes two paths to qualitative designation under Article 3(8): an "integrated intermediation" framework grounded in the two-sided economics of cloud and AI marketplaces, and an "indirect ecosystem capture" framework that extends the relevant end-user analysis to those drawn into hyperscaler ecosystems through downstream service consumption. Conditional on designation, it develops a remedial framework centred on "cloud neutrality" under Article 6(6), data obligations under Articles 6(2) and 6(9), and the application of Article 5(7)'s anti-tying obligation to hyperscaler identity and access management systems. The analysis engages directly with the European Commission's November 2025 dual-track investigations into AWS and Microsoft Azure.

Table of Contents

Preface

Cloud computing is crucial to Europe, not only as a technology sector but as the foundation of the data economy. It underpins nearly every sector and enables leadership in emerging technologies such as AI. Yet Europe's cloud market is dominated by a small number of very large overseas hyperscalers. Structural barriers, including market fragmentation, limited access to capital, and unintended consequences of EU regulation, prevent many European cloud providers, particularly SMEs, from fully competing.

In recent years, the Konrad-Adenauer-Stiftung has played an active role in addressing regulatory gaps and enforcement challenges related to digital gatekeepers. The underlying study by Antonio Manganelli represents our timely contribution to identifying workable solutions within the existing regulatory framework, namely the Digital Markets Act (DMA). The DMA was designed as a complement to competition law and aims to address structural market failures in the digital economy through ex ante regulation. Despite cloud computing services being explicitly listed as a core platform service, the regulation has remained largely inoperative in this sector.

This regulatory gap was formally acknowledged in November 2025, coinciding with the Digital Sovereignty Summit in Berlin, when the European Commission launched three market investigations. While these steps mark progress, they also reveal deeper structural tensions in applying the DMA to cloud markets.

At its core, the DMA is built around the economic model of the two-sided platform. Cloud computing, however, operates according to a fundamentally different logic, as this study clearly illustrates. Cloud services are organised as vertically integrated value chains, with infrastructure serving as an upstream input for downstream digital services.

Antonio Manganelli identifies concrete analytical shortcomings underlying this outcome and proposes corrective pathways that could contribute to a more contestable cloud economy in the European Union. The study outlines a remedial framework, conditional on gatekeeper designation, structured around complementary regulatory approaches, including data-related obligations, marketplace fairness rules, and, most notably, the principle of cloud neutrality.

Understanding where intermediation actually occurs, most prominently in cloud marketplaces, and addressing deeper forms of lock-in, including identity management systems, is essential to ensuring that the DMA achieves its objective of safeguarding fairness and contestability in the evolving digital economy. As Manganelli highlights, applying the DMA to cloud markets will require not only rigorous enforcement but also conceptual adaptation.

Without a competitive cloud sector, the European Union cannot achieve its objectives of digital sovereignty. With this publication, released on the occasion of the European Data Summit in Berlin, we aim to provide meaningful support to the work of the European Commission and other enforcement authorities across Europe.

Pencho Kuzev
Konrad-Adenauer-Stiftung e. V.

1. Introduction: Concentrated Cloud Markets and the Limits of Antitrust

Cloud computing markets are characterised by rapid structural expansion alongside significant and growing concentration. In Europe, growth rates have averaged approximately 25 to 30 per cent per annum over the past five years, and by 2023, approximately 52.7 per cent of EU companies with ten or more employees used at least one cloud service, a figure that has continued to rise.[1] In this scenario, the three largest cloud service providers – Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, collectively known as hyperscalers, account for approximately 70 per cent of revenues at the IaaS level.[2]

This concentration is neither contingent nor transient. This reflects the deep structural features of cloud markets, which systematically favour incumbents and raise durable barriers to entry and expansion. At the IaaS level, very high fixed and sunk costs for data centre construction, network infrastructure, and server equipment generate pronounced and persistent economies of scale. The resulting tendency towards an oligopolistic market structure is self-reinforcing: scale advantages in infrastructure translate into competitive advantages in adjacent services, and these advantages, in turn, attract the data volumes and workloads that further entrench the incumbents' cost and capability leads.[3]

Beyond the structural economics of concentration, market investigations by multiple national competition authorities in the Netherlands (ACM),

France (Autorité de la concurrence), the United Kingdom (Ofcom/CMA), and others[4] have consistently identified a set of conduct-based practices that further distort competition and lock customers into incumbents' ecosystems.[5] These include:

- *Technical barriers:* restrictions on data portability, closed APIs, and differentiated technical standards that make reconfiguration for alternative cloud environments costly and operationally disruptive

- *Organisational and procedural barriers:* absence of interoperability between providers, preventing effective multi-cloud deployment without significant re-engineering

- *Commercial barriers:* bundling and tying strategies that leverage market power from dominant adjacent markets – most notably productivity and enterprise software – into cloud infrastructure services

- *Economic and monetary barriers:* high and unpredictable egress fees, and large discounts on upfront spending commitments that create durable financial lock-in ("committed spend discounts")

It is essential to clarify the legal nature of these competitive concerns at the outset because it directly determines the appropriate regulatory instrument to address them. With the partial exception of Microsoft's software licencing practices[6], where the leveraging of dominance in productivity software into cloud infrastructure has been the subject of competition proceedings, these investigations have not been conducted as abuse of dominant position proceedings under Article 102 TFEU.[7] The reason is structural: cloud service markets exhibit an oligopolistic configuration in which no single provider holds an *individual* dominant position as required by Article 102 standards. Collective dominance remains theoretically available but has proven extremely difficult to establish under EU law, requiring demonstrable economic links between the allegedly colluding parties – a threshold that the heterogeneous competitive

dynamics among hyperscalers are unlikely to satisfy.[8] Therefore, antitrust law is structurally ill-equipped to address the competitive pathologies of cloud markets, not as a matter of enforcement failure, but as a matter of legal architecture.

This is precisely the gap that ex-ante regulation, specifically the Digital Markets Act (DMA)[9], was designed to fill as a complement to the competition law.[10] However, despite cloud computing services being expressly listed as a core platform service (CPS) in the DMA, the regulation has remained entirely inoperative in this sector. The Commission completed two rounds of gatekeeper designations, in June 2023 and October 2024, without designating any cloud service provider, leaving the market's structural and conduct-based pathologies entirely outside the regulation's remedial perimeter.[11]

In November 2025, the Commission opened three market investigations under the DMA: two to assess whether AWS and Microsoft Azure qualify for qualitative gatekeeper designation under Article 3(8), and a third to examine whether the existing DMA obligations are adequate to address fairness and contestability concerns in cloud markets. This dual-track initiative reflects the Commission's recognition that the challenge is simultaneously one of designation, i.e., who is subject to the regulation, and one of remedy adequacy, i.e., whether the available obligations, once triggered, are fit for purpose in the cloud context.

The two questions are analytically distinct but operationally inseparable: remedies can only be applied upon designation, and designation is therefore the legal and logical prerequisite for any regulatory intervention under the DMA. The following analysis therefore necessarily addresses both dimensions.

2. Gatekeeper Designation

2.1 Cloud Services and the DMA: The Platform-Pipeline Mismatch

2.1.1 The DMA's Platform Logic and Cloud's Vertical Pipeline Structure

The DMA is built around the concept of a two-sided platform as its central regulatory concept. Core platform services are characterised – as Recital 2 of the DMA explicitly notes – by "very strong network effects, the ability to connect many business users with many end users due to the multi-sided nature of these services." The gatekeeper concept translates this structural feature into an operational legal criterion: the requirement of being an "important gateway for business users to reach end users" (Article 3(1)(b) DMA), quantified by thresholds of 45 million monthly active end users and 10,000 active business users in the EU per year (Article 3(2)(b) DMA).

This architecture reflects the paradigmatic cases that motivated the DMA: online intermediation services, search engines, social networks, and app stores – markets where a large platform intermediates between two or more distinct user groups whose demands are interdependent. In these markets, the platform is the gateway: business users depend on it to reach consumers, and consumers access business users' services through it.

Cloud services follow a fundamentally different economic and commercial structure. Cloud computing delivers IT and computing resources, such as servers, storage, databases, software, networks, and data analytics, via the Internet, which is scalable on demand without requiring

customers to own or directly manage physical infrastructure. The IaaS-SaaS value chain is vertical, not two-sided; infrastructure is provided at the base layer, development platforms and tools in the middle layer, and applications at the apex. In this configuration, cloud providers stricto sensu do not act as intermediaries between two distinct user groups whose demands are interdependent. Instead, downstream business customers of IaaS services, independent software vendors (ISVs), and SaaS providers use cloud infrastructure as a productive upstream input to develop and supply their services to downstream consumers.[12] These business customers are access-seekers and potential downstream competitors of the vertically integrated cloud provider, which is structurally more analogous to the telecommunications access stack than to two-sided digital platforms.

2.1.2 The Gateway Problem: Business User and End User Misalignments

This vertical structure is the source of what is termed the "gateway problem" inherent in applying the DMA to cloud services. The structural mismatch between the platform logic of the DMA and the pipeline architecture of the cloud generates two distinct misalignments in the application of user definitions of the regulation.

Business users. The DMA provides a broad definition of business users: any person using a CPS "for the purpose of supplying goods or services to end users or in the course of carrying out such activity" (Article 2(21) DMA). For cloud services specifically, the Annex to the DMA defines business users as those providing "cloud computing services hosted in the cloud infrastructure of the relevant cloud computing service provider." This definition is sufficiently broad to accommodate access-seekers in a vertical chain: an ISV that uses a hyperscaler's IaaS to build and market a SaaS product qualifies as a business user even without performing any intermediation activity. Therefore, the definition is applicable.

However, its application to cloud markets could generate structural paradoxes. In a vertical pipeline, the number of business users primarily reflects the intensity of downstream competition, that is, the degree to which independent ISVs remain active on the platform, rather than the importance of the gateway function per se. A vertically integrated hyperscaler that has foreclosed independent ISVs from the market, and thereby reduced the number of active business users, would perversely be less likely to meet the designation threshold, and thus, less likely to be subject to regulatory obligations.

Further, more important qualifications are warranted in this respect. As the limited number of cloud competition cases makes evident, the leveraging dynamic in cloud markets has operated within the hyperscalers' ecosystem primarily in the *downstream-to-upstream* direction: large technology firms with dominant positions in software or consumer services – most notably Microsoft in productivity software, but also Amazon in e-commerce and Google in search, and the wider Google downstream ecosystem – leveraged their downstream customer bases to expand into upstream cloud infrastructure, in many cases initially offering infrastructure capacity at subsidised or no cost. This historical trajectory implies that the market power currently exercised at the IaaS layer has been structurally dependent on and reinforced by the continued dominance of downstream services. Therefore, the competitive relevance of each hyperscaler's IaaS layer cannot be assessed in isolation from its downstream ecosystem within which it is embedded. This is pivotal to what we will observe later in Section 2.2.

End users. This problem is more severe and directly fatal for quantitative designations at the end-user level. The Annex to the DMA defines active end users of cloud services as those who have "interacted with the cloud computing services of the relevant cloud computing service provider at least once during the month, in exchange for any type of remuneration." The verb "interact" and the remuneration requirement together establish that qualifying end users must have a direct economic and

commercial relationship with the candidate gatekeeper. This definitional requirement excludes the customers of ISVs, who access the upstream cloud infrastructure of the potential gatekeeper only indirectly through the ISV's own service. In a typical B2B cloud scenario, the end users of an ISV's SaaS product have no contractual or economic relationship with the underlying IaaS provider, as they contract with the ISV and are unaware of or indifferent to the infrastructure layer on which the application runs. The result is that the cloud provider's countable end-user base is limited to its own direct customers, which – particularly at the IaaS and PaaS levels, where clients are primarily sophisticated enterprise organisations rather than mass consumers – falls far below the 45 million monthly active end-user thresholds. This is the principal and proximate reason why no cloud provider met the quantitative criteria for designation across the two rounds of the Commission's gatekeeper determination process.

2.1.3 Consequences for Designation

The structural incompatibility between cloud's vertical architecture and the DMA's platform-based design explains why no cloud service provider has been designated after two rounds of gatekeeper designation in June 2023 and October 2024. The quantitative shortfall of end users is not a contingent empirical gap that will close as cloud adoption grows; rather, it is a structural consequence of the definition. The more cloud services are consumed through ISV-mediated deployments rather than through direct enterprise contracts, the wider the gap between the DMA's end-user count and any economically meaningful measure of market reach or impact.

Moreover, the qualitative route under Article 3(8) does not resolve this difficulty. A purely qualitative designation requires establishing, without reliance on quantitative presumptions, that AWS and Microsoft Azure each (i) have a significant impact on the internal market, (ii) constitute

an important gateway for business users to reach end users, and (iii) enjoy a deep-rooted and lasting economic position in cloud services. Of these three criteria, the first and third are clearly satisfied based on the market share, revenue scale, and structural barriers to entry described in Section 1. Instead, the "important gateway" criterion is a critical legal obstacle that cannot be severed from the conceptual architecture of the DMA's platform logic.

The qualitative criteria of Article 3(8) – network effects, scale and scope economies, data advantages, user lock-in, conglomerate structure, and vertical integration – are not themselves a substitute for the gateway function. Rather, they are indicators of the importance of an existing gateway: they explain why a platform that already functions as a gateway is likely to entrench and consolidate that position. However, they cannot construct a gateway function in a service configuration where intermediation between business users and end users is structurally absent or attenuated.[13]

A qualitative assessment that relies solely on these economic characteristics without conceptually establishing the underlying gateway relationship would conflate market power with the specific regulatory concept of gatekeeping that the DMA is designed to address. The Commission's November 2025 investigations into the qualitative designation of AWS and Microsoft Azure, which emphasise lock-in, vertical integration, and conglomerate structure, will need to confront this conceptual gap directly if they are to produce a legally robust designation outcome. The next section 2.2 will start addressing this complex and pivotal issue.

2.2 Possible Paths to Designation

2.2.1 The Cloud Marketplace as a Two-Sided Layer

The standard vertical pipeline analysis of cloud services requires qualification in one economically and commercially significant respect: cloud marketplaces. All three major hyperscalers operate dedicated marketplace services – AWS Marketplace, Azure Marketplace, and Google Cloud Marketplace – through which customers can discover and purchase not only the hyperscaler's own services but also PaaS and SaaS products developed and marketed by ISVs and other third-party providers. When operating in this capacity, hyperscalers introduce genuine two-sided platform economics into the cloud services market: they intermediate between the supply side (ISVs as business users) and the demand side (enterprise customers and, increasingly, end consumers as end users), coordinating the interaction between these two groups and deriving value from it.[14]

In this configuration, the conditions for the DMA gateway function are satisfied substantively and analytically. ISV business users depend on the marketplace to reach customers across the hyperscaler's installed user base; the marketplace's demand side encompasses both enterprise clients and end consumers with a direct commercial and contractual relationship with the marketplace operator.

In this context, even if the quantitative thresholds may not be met, the qualitative assessment of the gateway function becomes analytically coherent and operationally tractable: the marketplace generates the bilateral interdependence structure that the DMA's gatekeeper concept is designed to regulate. For qualitative designation purposes under Article 3(8), the presence of network effects, scale economies, and user lock-in within the marketplace layer provides substantive justification for the important gateway finding, independently of whether the quantitative thresholds are formally triggered or not.

The emergence of AI Foundation Model (FM) marketplaces operated by hyperscalers further reinforces this analysis. Amazon Bedrock, Microsoft Azure AI Foundry, and Google Vertex AI each intermediate between FM developers and deployers, as business users, and the downstream firms or consumers who access AI-powered applications as end users. These platforms combine a marketplace intermediation layer with deep integration into the underlying cloud infrastructure required for inference computing, model fine-tuning, and deployment orchestration. Thus, they exhibit the same structural characteristics as cloud product marketplaces, amplified by the strategic importance of AI infrastructure as an upstream input across the entire AI value chain, a consideration that significantly strengthens the qualitative case for the gateway function and entrenched position.[15]

2.2.2 Integrated Intermediation as a Specification of Ecosystem Power

In addition, cloud and AI marketplace activities are not equivalent to a standalone intermediation service, such as Booking.com or even the Amazon marketplace, and should not be analysed as such. It is qualitatively distinct because of the highly integrated character of the intermediation: hyperscalers are simultaneously (i) the upstream infrastructure provider – IaaS – on which ISVs build their products; (ii) the marketplace intermediary through which those products are distributed and sold; and (iii) direct downstream competitors offering their own competing SaaS, PaaS, and FM products through the same marketplace. This multiple integration can be captured by the concept of "integrated intermediation", which is proposed as a specification and extension of ecosystem power in the cloud context.

Ecosystem power is analytically relevant to the qualitative criteria for gatekeeper designation, particularly when the quantitative thresholds are not met.[16] Indeed, the DMA's Article 3(8) qualitative assessment

expressly references network effects, scale and scope economies, user lock-in, data advantages, and the conglomerate corporate structure or vertical integration of the undertaking. Integrated intermediation translates these abstract criteria into a concrete and tractable characterisation of the gateway function in cloud markets: the hyperscaler controls access to the marketplace for ISV business users; controls the upstream infrastructure inputs that the same business users depend on to build and run their products; and simultaneously competes with them at the application layer. This configuration generates dependencies and foreclosure risks that are structurally more severe than those of a pure intermediation platform, precisely because the gatekeeper's power extends vertically across the entire value chain rather than being confined to the intermediation layer itself.

From a designation perspective, the legally cleanest path may be to treat cloud and AI marketplace activity as a distinct CPS, specifically as an online intermediation service, rather than, or in addition to, "cloud computing services" per se. The DMA's definition of online intermediation services (Article 2(2)) encompasses services that allow business users to offer goods or services to consumers, which marketplace activity plainly satisfies. Under this approach, the designation would target the marketplace layer directly, while the underlying cloud infrastructure would be brought within the regulatory perimeter through an integrated structure of the applicable obligations.

Alternatively, if cloud service CPS remains the designation basis, the Annex definitions of business users and end users should be revisited to reflect marketplace reality – an amendment that the DMA currently permits through delegated acts under Article 3(9). Either route requires recognising, as a foundational analytical matter, that the gateway function in cloud markets operates primarily through the marketplace and intermediation layer, not through the pipeline layer.

2.2.3 Indirect Ecosystem Capture: A Further Path to the Gateway Function

A further and complementary path to establishing the gateway function in a qualitative assessment arises from the downstream-to-upstream leveraging dynamic that has characterised the competitive history of hyperscaler expansion. As illustrated most clearly by Microsoft productivity software investigations, market power in cloud markets has not typically generated at the infrastructure layer and then extended downward. Rather, the dominant trajectory has been the reverse: large technology firms with entrenched downstream positions (in productivity software, e-commerce, or consumer services) leveraged those positions to build or expand upstream into cloud infrastructure, frequently by offering infrastructure services at subsidised or no cost to downstream customers in the early phase of market development. The IaaS position of today's hyperscalers is, in significant part, a consequence and extension of downstream dominance.[17]

This historical trajectory has a structural implication that is directly relevant to the gateway analysis. When a customer chooses a SaaS application provided by a hyperscaler, that choice implicitly and often invisibly carries a choice of the hyperscaler's broader cloud ecosystem, including its underlying IaaS infrastructure.

The end user who adopts Microsoft 365 does not consciously select Azure as their cloud infrastructure provider; however, the integrated architecture of Microsoft's service stack makes that outcome operationally and commercially probable and, in many enterprise deployments, near inevitable. The analogy with the mobile and fixed operating system ecosystems is instructive: the end user who purchases a smartphone does not formally choose the mobile OS; however, that choice is an inescapable structural consequence of the handset decision. The OS constitutes an indirect but determinate choice embedded in and inseparable from consumer-facing product decisions.

A similar logic applies to hyperscaler cloud ecosystems. In this framework, the relevant end-user base for the qualitative gateway function is not confined to those who have a direct contractual relationship with the hyperscaler's IaaS or PaaS services, which is the narrow definition that produces the end-user counting problem identified in Section 2.1. It extends to all those who are drawn into the hyperscalers' cloud ecosystems by virtue of consuming their downstream services, and for whom the choice of cloud infrastructure is a structural consequence of that downstream consumption.

These are the end users who have generated the scale, data volumes, network effects, and conglomerate advantages that the Article 3(8) qualitative criteria seek to capture. Indeed, recital 32 refers those characteristics to contestability issues for the core platform services and the related ecosystem.[18] A qualitative gateway assessment that ignores this indirect ecosystem population, which may be orders of magnitude larger than the direct IaaS customer base, systematically understates the economic and competitive significance of the hyperscaler's position and produces a finding that is analytically incomplete.

This reading also provides a more principled basis for the Article 3(8) qualitative assessment than a simple enumeration of economic characteristics. It establishes that the gateway function exists – not at the IaaS pipeline layer, where intermediation is structurally absent, but at the ecosystem level, where the hyperscaler's integrated position across downstream services and upstream infrastructure makes it the *de facto* gateway through which a substantial and expanding population of users and enterprises are organised into a single cloud ecosystem. The economic characteristics listed in Article 3(8) – network effects, lock-in, scale economies, vertical integration, and conglomerate structure – then operate as intended: as evidence of the depth, durability, and entrenchment of a gateway function that is already structurally established.

3. Applicable Remedies

Designation is a prerequisite for any DMA obligations. The analysis of remedies in this section is therefore conditional on designation, whether through the qualitative assessment of AWS and Microsoft Azure currently under investigation or through a marketplace-based designation route, as discussed above. Given this condition, we identify the most relevant and potentially impactful DMA obligations, organised around three distinct but complementary regulatory logics: the cloud neutrality principle grounded in Article 6(6); data-related obligations under Articles 6(2) and 6(9); marketplace-specific obligations addressing intermediation fairness; and the possible untying of identification systems.

3.1 A Case for "Cloud Neutrality"

3.1.1 Article 6(6): Principles and Scope

Article 6(6) of the DMA requires that designated gatekeepers neither prevent nor restrict business users from offering the same products or services to end users through different channels on different terms, and neither technically restrict switching or multi-homing nor degrade the conditions of access or use for business users who multi-home or switch. In the cloud context, this provision carries a scope and significance that substantially exceeds its literal application in other CPS contexts.

Three features of this provision are analytically significant for cloud regulation. First, the prohibition is deliberately technology-neutral: it applies to restrictions that are "technical or otherwise", encompassing

both architectural barriers (API incompatibility, proprietary formats, closed middleware) and commercial or contractual barriers (differential pricing, licensing surcharges, egress fee structures), without requiring a distinction between them. Second, the provision protects end users' ability to switch between different software applications and services and subscribe to multiple applications and services simultaneously, thus covering both sequential switching and concurrent multi-homing within a single framework. Third, the core platform service is identified as the vehicle of access through which end users reach software applications. In the cloud context, this vehicle is the IaaS infrastructure layer itself, which positions that layer as the regulated bottleneck for the purpose of the obligation.

Indeed, from the perspective of a customer who accesses multiple SaaS applications, some provided by the hyperscaler itself and others by ISVs, through a single cloud infrastructure environment, that infrastructure functions as an access layer which constitutes a platform through which end users (directly) and ISVs (as intermediaries to their downstream customers) access software applications and services. Article 6(6) was expressly applied in the DMA to operating systems for precisely this reason: the gatekeeper's control of the OS layer gives it the technical and commercial ability to restrict or distort end users' access to competing applications. The same logic applies to cloud infrastructure upon designation. A hyperscaler's control of the IaaS/PaaS layer gives it the ability to restrict end users' and ISVs' access to competing SaaS applications, impede portability between cloud environments, and make switching between or multi-homing across cloud providers technically or commercially prohibitive, i.e., the precise harm that Article 6(6) is designed to prevent.

3.1.2 The Cloud Neutrality Concept

Article 6(6) is currently among the least extensively utilised DMA obligations; however, it has the potential to be one of the most powerful instruments for opening digital markets to competition. In the cloud context, where the dominant market structure is a vertical pipeline rather than a consumer-facing platform, an analogy with net neutrality under the Open Internet Regulation (OIR)[19] is both analytically productive and normatively compelling.

Under the OIR, Internet Service Providers are prohibited from discriminating among Content and Application Providers in the provision of Internet access services: all CAPs must be able to reach end users on equal terms, without degradation, blocking, or differential treatment by the network layer.[20] The underlying normative logic is that the infrastructure layer must remain neutral with respect to the application layer that builds on top of it – not exploiting control over the network to favour affiliated applications or economically exploit downstream applications providers.

This logic could be adopted (and adapted) to the cloud infrastructure. A vertically integrated hyperscaler, designated as the gatekeeper, controls the IaaS/PaaS infrastructure that ISVs use as an upstream productive input. Cloud users – both end users and business users – should "have the right to access and distribute information and content, use and provide applications and services."[21] Article 6(6), rigorously interpreted, could precisely discipline these aspects: it requires a designated gatekeeper to treat all business users who use the infrastructure to build and deliver competing downstream applications on equal and non-discriminatory terms, at the same time providing end users specular access rights. This could be labelled as the substantive concept of "cloud neutrality": the obligation on the cloud infrastructure layer not to discriminate among the applications and services deployed on top of it.

However, there is an important structural difference between net and cloud neutrality, which makes the latter a more complex regulatory challenge. Net neutrality was designed to constrain ISPs that, as access bottlenecks, could exercise market power against content providers seeking to reach end users: this is a bilateral and directionally clear relationship. Cloud neutrality concern operates in both directions along the vertical value chain simultaneously: the hyperscaler exercises market power upstream as an IaaS provider to ISVs who are its own SaaS competitors, and downstream as a SaaS provider to end users who are simultaneously the customers of those ISV competitors. Therefore, the self-preferencing dynamic is structural and operates in vertical and horizontal dimensions simultaneously, which is a more complex and deeply embedded regulatory challenge than the ISP/content-provider bilateral relationship that OIR net neutrality was designed to address.

Therefore, for the purposes of Article 6(6), the relevant population of protected parties must be interpreted broadly and consistently with the analysis of the cloud ecosystem in Section 2.2 above. The provision's protections extend to direct cloud customers (i.e., customers who access SaaS applications through the cloud infrastructure under a direct contractual relationship with the hyperscaler), to ISVs as business users whose ability to reach their end customers is conditioned or restricted by the hyperscaler's control of the access infrastructure, and, critically, also to ISVs' customers.

This extension is supported by the DMA's definitional framework. In Article 2(21), business users are defined as any person using a CPS "for the purpose of or in the course of providing goods or services to end users": this captures ISVs precisely, since they use cloud CPS infrastructure as the technical means of providing SaaS services to their downstream customers. In turn, those downstream customers may themselves qualify as end users within the meaning of Article 2(20) DMA – "any natural or legal person using core platform services other than as a business user" – a definition broad enough to encompass persons who interact with a CPS

indirectly, through the intermediation of a business user, in the vertical pipeline structure characteristic of cloud service delivery.[22]

3.1.3 From Cloud Neutrality to Equivalence of Access

In this context, an extensive and rigorous application of Article 6(6) – in particular, through the specification mechanism of Article 8 DMA, which allows the Commission to further define and tailor obligations for specific core platform services – would produce a result functionally equivalent to an equivalence of access remedy applied in vertical pipelines regulatory frameworks.

For example, in the electronic communications regulation, a vertically integrated operator with significant market power is required to offer upstream access services to downstream competitors on terms identical (equivalence of inputs) or at minimum comparable (equivalence of outputs) to those it applies to its own downstream operations – same price, same technical conditions, same processes, and timelines.

Translated to cloud services, an Article 6(6)-based equivalence of access obligation would require a designated gatekeeper to offer IaaS/PaaS infrastructure access to ISVs on economic, commercial and technical terms no less favourable than those applicable to its own downstream PaaS and SaaS operations. This would prohibit quality degradation, preferential internal pricing, or differential service levels that systematically disadvantage independent providers relative to the gatekeeper's own competing services.

3.1.4 FRAND Access: Extending Article 6(12)

Finally, Article 6(12) of the DMA requires designated gatekeepers to provide business users with access to certain core platform services, specifically app stores, online search engines, and online social networking services, on fair, reasonable, and non-discriminatory (FRAND) terms. In its current form, this provision does not apply to cloud computing services as a CPS, even after designating a cloud provider as a gatekeeper.

This limitation is difficult to justify, considering the access dynamics identified. If a designated cloud gatekeeper controls an infrastructure that business users depend on as an upstream productive input, FRAND access obligations are at least as warranted as they are in the app store context, where third-party developers depend on the distribution platform in a structurally analogous manner.

Two routes are available to address this gap. The first and most direct is a legislative amendment extending Article 6(12) to cloud computing services – a change that would be fully consistent with the objectives of the November 2025 market investigation into the effectiveness of existing DMA obligations in cloud markets, which may result in a delegated act under Articles 12 and 49 DMA or in a legislative proposal under the DMA's review clause. The second is a functional route: an extensive interpretation of Article 6(6), developed through a Commission specification under Article 8, could produce a result substantially equivalent to FRAND access by requiring that the terms, pricing, and conditions of infrastructure access be fair, reasonable, and non-discriminatory – effectively importing the FRAND standard through the cloud neutrality and non-discrimination route.

3.2. Further Applicable Obligations: Data, Intermediation Fairness, and Identity Management

The cloud neutrality framework developed in Section 3.1 addresses the infrastructure layer dimension of competitive harm in cloud computing markets. However, it does not exhaust the regulatory toolkit available upon designation. Three further clusters of DMA obligations bear directly on the contestability and fairness issues of cloud markets identified in Section 1: the anti-tying obligation of Article 5(7), addressing the control of identity and authentication infrastructure as a structural source of ecosystem lock-in; data-related obligations under Articles 6(2) and 6(9), addressing the extraction and exploitation of business-user data and the barriers to portability and switching; and marketplace-specific obligations addressing intermediation fairness in the context of integrated cloud and AI marketplaces.

3.2.1 Identity Management and Article 5(7) Anti-Tying Obligation

A further provision of immediate operative relevance upon designation is Article 5(7) DMA, which prohibits designated gatekeepers from requiring end users or business users to use, offer, or interoperate with an identification service, web browser engine, or payment service of the gatekeeper in the context of services provided by business users using the core platform service of the gatekeeper. Its operative logic is anti-tying: it prevents gatekeepers from conditioning access to, or effective use of, their CPS on the adoption of a second, ancillary service that the gatekeeper controls, thereby extending and entrenching the gatekeeper's competitive reach beyond the primary platform relationship.

This provision may be particularly significant in the cloud context because of the structural role that identity and access management (IAM) systems play across the cloud ecosystem. All three major hyper-

scalers operate proprietary IAM services – Microsoft Entra ID (formerly Azure Active Directory), AWS Identity and Access Management, and Google Cloud Identity – that govern authentication, authorisation, and access policy across the entirety of an organisation's cloud-hosted environment. This means that IAM services, coupled with cloud infrastructure, are gateways to all applications, including AI tools.

These systems are not peripheral or ancillary tools: they constitute the administrative control plane through which every resource, service interaction, and user access event within the cloud environment is managed and enforced. An enterprise deploying workloads on Azure or AWS must configure its access management environment using the provider's native identity service for practical and architectural purposes. Third-party identity providers, such as Okta or Ping Identity, may be integrated to a degree at the application layer, but the underlying IAM fabric, particularly for infrastructure-layer authentication and resource access policy enforcement, remains tightly and often inseparably coupled to the hyperscaler's proprietary system.

Consequently, the identity layer is one of the most durable and operationally significant sources of switching barriers in cloud markets: a form of lock-in that is structurally independent of, and potentially more resilient than, data portability barriers or egress fee structures, and that operates at a layer of the infrastructure below and prior to the services that portability and switching remedies address.

The central interpretive question regarding the application of Article 5(7) to cloud IAM is whether enterprise IAM systems qualify as an identification service within the meaning of the provision. The DMA does not provide a standalone definition for this term. Recital 43 frames the provision around services that are "crucial for business users to conduct their business" and that, if required by the gatekeeper, provide it "a means of capturing and locking-in new business users and end users."

The recital was drafted with consumer-facing SSO mechanisms as the paradigmatic target (e.g., “Sign in with Google”, “Sign in with Apple”) where a consumer application developer required to implement the gatekeeper’s login service as a condition of platform access cannot substitute that service without rebuilding the authentication architecture of its application. However, the functional logic seems to map directly and with equal analytical force onto enterprise cloud IAM: a business user deploying infrastructure on a hyperscaler’s platform and required to manage access through the hyperscaler’s native identity service faces an identical structural constraint, arguably more severe in its operational and financial dimensions. Thus, migrating to a competing cloud provider entails not only data portability but also a complete re-architecture of the organisation’s identity estate, such as user directories, role hierarchies, access policies, service principal configurations, and federated identity integrations.[23]

The Article 5(7) obligation and the cloud neutrality principle of Article 6(6) are not merely cumulative: they are structurally complementary in a significant sense. Article 6(6) operates at the infrastructure access layer, by governing the terms under which competing applications and services can be deployed and accessed through the cloud platform. Article 5(7) operates at the identity and authentication layer, which is logically and architecturally prior to the application access, and governs the conditions under which users and services can be recognised, verified, and authorised within the cloud environment. Together, these two provisions address the two principal architectural layers through which hyperscaler lock-in could be engineered and maintained: infrastructure access and identity control.

3.2.2 Data Obligations: Articles 6(2) and 6(9)

Article 6(2) prohibits designated gatekeepers from using, in the context of any service they provide, data generated by the activities of their business users – including data generated in the course of or in relation to the use of the relevant CPS – for the purpose of competing with those business users.[24] Recital 48 of the DMA provides an explicit cloud-specific interpretation of this obligation, specifying that it extends to "data provided or generated by business users of the gatekeeper in the context of their use of the cloud computing service of the gatekeeper, or through its software application store that allows end users of cloud computing services access to software applications." In practice, this means that a designated hyperscaler cannot use data generated by ISVs' deployment of services on its cloud infrastructure, such as performance metrics, usage patterns, configuration data, API call logs, and customer behaviour data, to improve, develop, or inform the positioning of competing cloud or non-cloud services.

Market evidence confirms the practical salience of this obligation in vertically integrated platform ecosystems, for example, in situations where gatekeepers can extract competitive intelligence from third-party sellers on their e-commerce marketplace to develop competing own-brand products, illustrating the structural incentive for data exploitation. The same incentive structure is present, arguably in an amplified form, in the cloud infrastructure context, where the gatekeeper hosts and has near-total visibility into a broad range of ISVs/downstream services.

In addition, Article 6(9) requires designated gatekeepers to ensure the effective portability of data generated by end users' and business users' activities in real time and free of charge through interoperable technical means. In the cloud context, this obligation would require designated providers to ensure that workloads, PaaS and SaaS deployments, configurations, and associated data assets can be fully ported to competing cloud environments without egress fees or technical impediments. The

interaction between Article 6(9) and the EU Data Act is analytically important. The Data Act establishes a detailed and symmetric framework of switching and portability obligations applicable to all cloud service providers under Chapters VI and VIII, providing a baseline standard of portability and interoperability that applies irrespective of gatekeeper status. The DMA's Article 6(9) obligations, being asymmetric and applying only to designated gatekeepers, must be interpreted as at least as demanding as the symmetric Data Act baseline.[25] The Commission's Article 8 specification power provides the mechanism through which the content of Article 6(9) obligations can be elaborated and calibrated to the specific characteristics of cloud portability in a manner that ensures genuine, operationally effective switching rather than nominal compliance.

3.2.3 Marketplace-Specific Obligations: Intermediation Fairness

Where designation proceeds on the basis of, or in relation to, cloud marketplace activity – whether as online intermediation services under Article 2(2) or as a cloud CPS with integrated intermediation characteristics, as argued in Section 2.2 – the full suite of DMA provisions governing intermediation fairness becomes applicable. These provisions address competitive harms that are specific to the integrated intermediation structure: the gatekeeper's ability to exploit its simultaneous position as upstream infrastructure provider, marketplace intermediary, and downstream competitor to favour its own services and disadvantage ISVs.

The most directly applicable provisions are as follows. Article 5(3) prohibits the designated gatekeeper from requiring ISVs to offer their products on the marketplace on terms no less favourable than those offered on other distribution channels. This is a prohibition directly relevant should hyperscaler marketplaces impose most-favoured-nation conditions on ISV pricing, thereby restricting ISVs' ability to compete on price outside the marketplace and reinforcing the gatekeeper's distribution

control. Article 5(4) requires the gatekeeper to allow business users to communicate with and redirect their customers to off-marketplace channels and to conclude contracts outside the marketplace without restriction, thus addressing the anti-steering practices that prevent ISVs from building direct customer relationships and creating permanent dependency on the marketplace distribution layer. Article 5(5) requires the gatekeeper to allow end users to access and use business users' services acquired outside the marketplace through the marketplace interface, preventing the technical disintermediation of off-marketplace purchasing relationships and ensuring that customers who have contracted directly with ISVs can nonetheless access those services through the cloud environment. Finally, Article 6(5) prohibits the designated gatekeeper from self-preferencing its own downstream services in the ranking, presentation, or conditions of access on the marketplace relative to competing ISV services.

4. Conclusions

The application of the Digital Markets Act to cloud computing markets has been impeded since the regulation's entry into force by a structural incompatibility that this paper has sought to diagnose and address. This incompatibility is not incidental, but reflects the DMA's foundational design choice to model regulatory intervention on the two-sided intermediation platform – at a time when cloud infrastructure had not yet emerged as the defining competitive bottleneck of the digital economy. The result is a regulation that lists cloud computing services as a core platform service, acknowledges their strategic importance to fairness and contestability in digital markets, yet provides a designation framework so closely calibrated to consumer-facing two-sided platforms that it structurally excludes the providers it nominally covers.

The paper has identified three distinct analytical failures that explain this outcome and, in so doing, has proposed three corresponding correctives. First, the quantitative designation mechanism is structurally unfit for the cloud context. The cloud provider's countable end-user base reflects only its direct enterprise clients, not the vastly larger population of consumers and businesses whose digital environment is organised, mediated, and constrained by hyperscaler infrastructure through independent software vendor-mediated service deployments. This is unlikely to be an empirical gap that will narrow as cloud adoption grows.

Second, this paper proposes two paths through which the qualitative designation route under Article 3(8) can be legally grounded without circumventing the DMA's conceptual architecture. The first is the integrated intermediation framework: cloud and AI marketplaces operated

by hyperscalers introduce genuine two-sided platform economics into the cloud market, creating a bilateral dependency structure between ISV business users and enterprise or consumer end users that satisfies the gateway criterion and supports a coherent qualitative designation of the marketplace layer. The second is the indirect ecosystem capture framework: the downstream-to-upstream leveraging dynamic that has characterised hyperscaler expansion means that a substantial and economically significant population of end users is drawn into the hyperscaler's cloud ecosystem as a structural consequence of consuming its downstream services, without any direct contractual relationship with the IaaS layer. A qualitative gateway assessment that confines itself to direct contractual relationships systematically understates the competitive significance of the hyperscaler's position and produces analytically incomplete findings.

Third, this paper attempted to develop a remedial framework conditional on designation, organised around three complementary regulatory logics. The cloud neutrality principle, grounded in Article 6(6), translates the normative logic of net neutrality into the cloud infrastructure context: the IaaS/PaaS layer must remain neutral with respect to the application and service layer built on top of it, not exploiting their position. This principle provides the operational content of cloud neutrality as a non-discrimination and equal access obligation. Data-related obligations under Articles 6(2) and 6(9) – reinforced and calibrated against the Data Act's symmetric portability baseline – address the extraction of ISV operational intelligence and barriers to workload portability and switching. Marketplace-specific obligations under Articles 5(3), 5(4), 5(5), and 6(5) address the intermediation fairness dimension of the integrated structure.

A conceptually novel element of the remedial analysis, addressing the deepest layer of cloud lock-in, is the application of Article 5(7)'s anti-tying obligation to hyperscaler IAM systems. Its application to enterprise IAM upon designation would address a form of lock-in that operates below and prior to the layers addressed by data portability and switching obli-

gations. Along with Article 6(6)-based cloud neutrality, it could address the two principal architectural layers through which hyperscaler ecosystem control is engineered and maintained.

1 Eurostat, Cloud computing – statistics on the use by enterprises, December 2023, dataset isoc_cicce_use, available at: ec.europa.eu/eurostat/statistics-explained (last accessed: 23.03.2026).

2 Authority for Consumers and Markets [ACM] (2022), Market study into cloud services: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf (last accessed: 23.03.2026); Synergy Research Group, European Cloud Providers' Local Market Share Now Holds Steady at 15%, July 2025, available at: srgresearch.com (last accessed: 23.03.2026).

3 Manganelli, A., Schnurr, D. (2024), Competition and Regulation of Cloud Computing Services – CERRE Report, available at: https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf (last accessed: 23.03.2026); Crémer, J., Biglaiser, G., Mantovani, A. (2024), The Economics of the Cloud, Tse Working Papers 24-1520; OECD (2025), Competition in the Provision of Cloud Computing Services, OECD Roundtables on Competition Policy Papers, no. 323, https://doi.org/10.1787/595859c5-en.

4 See Manganelli, A. (2025), Policy Responses to competition concerns in Cloud and Competition Policy, Part V, Concurrences N° 8-2025, Art. N° 127472.

5 CMA (2025), Cloud Infrastructure Services – Final Decision Report, available at: https://www.gov.uk/cma-cases/cloud-services-market-investigation (last accessed: 23.03.2026); Ofcom (2023), Cloud Services Market Study; Autorité de la Concurrence (2023), Opinion 23-A-05 on the draft law to secure and regulate the digital space, available at: https://www.autoritedelaconcurrence.fr/fr/avis/concernant-le-projet-de-loi-visant-securiser-et-reguler-lespace-numerique (last accessed: 23.03.2026); ACM (2022).

6 The CMA has paid particular attention to Microsoft's software licensing practices, finding that the company has both the ability and the incentive to exclude competitors by making it less attractive – technically and commercially – for customers to use its products on rival cloud infrastructures [CMA, Cloud Infrastructure Services – Final Decision Report, 2025]. Similar concerns prompted Alphabet (Google) to file a complaint with the European Commission in September 2024, subsequently withdrawn in November 2025 in anticipation of the market investigation on cloud services and the DMA. In the United States, the FTC – as part of an already ongoing antitrust investigation – sent Microsoft an extensive request for information in November 2024, further accelerating proceedings in February 2026 by issuing Civil Investigative Demands (CIDs) to at least six companies competing with Microsoft in the business software and cloud markets.

7 For example, the CMA's action, based on the Enterprise Act 2002 (as amended by the Enterprise and Regulatory Reform Act 2013), is aimed at establishing an "adverse effect on competition" (AEC), whereas abuse of a dominant position – which requires the preliminary finding of a dominant position, whether individual or collective – is a distinct cause of action under the Competition Act 1998.

8 The Court of Justice has indeed held that "a dominant position may be held by two or more economic entities that are legally independent of one another, provided that, from an economic point of view, they present themselves or act together on a specific market as a collective entity" and that these entities will hold a dominant position "if there exist between the undertakings concerned economic links which enable them to act together independently of their competitors, their customers and consumers" (CJEU, 16 March 2000, Compagnie Maritime Belge Transports, joined cases C-395/96 P and C-396/96 P, §§ 36 and 42). The Commission's practice in the area of collective dominance has historically been very limited, and the few cases worth noting have typically concerned situations involving strong structural links between the undertakings presumed to hold a collective dominant position (CJEU, 7 October 1999, Irish Sugar, T-228/97).

9 Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

10 DMA Recital 10; and Manganelli, A., Nicita, A. (2022), Regulating digital markets; Robertson, V. (2024), The complementary nature of the Digital Markets Act and the EU antitrust rules, Journal of Antitrust Enforcement, vol. 12, no. 2, pp. 325–330; De Streel, A. (2020), Digital Markets Act: Making economic regulation of platforms fit for the digital age – CERRE Report.

11 Manganelli, A. (2025) (4).

12 Manganelli, A., Schnurr, D. (2024) (3); Bania, K., Geradin, D. (2024), The regulation of cloud computing: why the European Union failed to get it right, INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, vol. 33, no. 1, pp. 99–113.

13 Feasey, R. (2022), Note on designation of gatekeepers in the digital markets act – CERRE Issue Paper.

14 Manganelli, A., Schnurr, D. (2024) (3).

15 Manganelli, A. (2026), Foundation models and generative AI applications: what competitive concerns? European Competition Journal, available at: https://www.tandfonline.com/doi/full/10.1080/17441056.2026.2641378 (last accessed: 23.03.2026).

16 The DMA does not consider the ecosystem dimension as a necessary condition to apply regulation. See, Van den Boom, J., Hornung, P. (2025), Ecosystems in DMA designation decisions – Bridging the gap between legal text and economic reality, Journal of European Competition Law & Practice, vol. 16, no. 1, pp. 3–19. Nevertheless, the ecosystem concept is neither useless nor unimportant for the DMA. It is mentioned in key recitals describing the rationale and motivation of the regulation (recital 3), and thus it works as an interpretative tool, orienting interpretation of DMA's provisions in order to achieve its overall objectives. The relevance of ecosystem aspects is also related to where the orchestration activity take place in the value chain, as the more the orchestration activity is placed upstream in the value chain the more problematic it is, since it "controls" much more segments of the ecosystem and much more players.

17 The fact that cloud upstream markets are tight oligopolies is indeed a consequence of the leveraging of market positions from different dominated downstream markets.

18 "The features of core platform services in the digital sector, such as network effects, strong economies of scale, and benefits from data have limited the contestability of those services and the related ecosystems."

19 Regulation (EU) 2015/2120 laying down measures concerning open internet access.

20 See Manganelli, A. (2024), Toward ne(x)t neutrality. A Re-thinking of the EU open Internet Regulation, Media Laws, n 3/24, available at: https://www.rivistadidirittodeimedia.it/wp-content/uploads/2025/03/3-24-Manganelli.pdf (last accessed: 25.03.2026).

21 Art 3(1) OIR.

22 It should be noted that the definitions of "end users" and "business users" provided in the Annex to the DMA are operationally tailored to the quantification of the thresholds under Article 3(2) and are therefore functional to the quantitative designation process rather than being general conceptual definitions. Accordingly, in the context of interpretation and application of the DMA's obligations and remedies, the general definitions set out in Article 2(20) and Article 2(21) are applicable.

23 Cloud switching and the use of multi-cloud are generally disciplined by the Data Act – Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). However, this issue is not addressed.

24 See BEREC (2025), BEREC response to the European Commission's consultation on the first review of the Digital Markets Act, BoR (25)119.

25 Manganelli, A., Schnurr, D. (2024) (3).

The Author

Antonio Manganelli is Professor of Competition Law and Policy at the University of Siena and Research Fellow at the Centre on Regulation in Europe (CERRE). His research focuses on market structure, regulatory design, and institutional dynamics in telecoms, audiovisual, and digital markets, with a current focus on the application of competition law and policy to cloud computing and AI markets. He has previously carried out applied research for the European University Institute, the University of Rome LUMSA, the OECD, and the Bank of Italy's Research Department.

He brings to his academic work over 20 years of hands-on experience in European public institutions, having held senior positions at the Italian Communications Authority (AGCOM), the UK Competition and Markets Authority (CMA), the BEREC Office, and the Cabinet of the Italian Ministry of Economic Development.

Imprint

Published by: Konrad-Adenauer-Stiftung e. V., 2026, Berlin, Germany

Contact:
Dr Pencho Kuzev
Policy advisor Data and Competition Policy
Economy and Innovation/Analysis and Consulting
pencho.kuzev@kas.de
p +49 30 26996 3247

Cover page image: yellow too Pasiek Horntrich GbR
Design and typesetting: Konrad-Adenauer-Stiftung e. V.
Printed by: Kern GmbH, Bexbach, Germany
Printed in Germany.

This publication was published with financial support of the Federal Republic of Germany.

ISBN 978-3-98574-351-3

This policy paper examines why the Digital Markets Act (DMA) has struggled to apply to cloud markets, identifying a structural and regulatory mismatch between its platform-based design and the realities of cloud computing. It proposes new approaches to designation, focusing on cloud marketplaces and ecosystem dynamics. The study also outlines a forward-looking regulatory framework centred on cloud neutrality, data access, and fairness. By bridging legal design and market reality, it aims to provide practical guidance for the European Commission and other enforcement agencies to ensure enhanced contestability and fairness in the cloud economy.

Konrad-Adenauer-Stiftung e. V.