ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

ECIPE Policy Brief – No. 07/2026

Europe's Digital Markets Act Under Review: Ways to Make it More Pragmatic, Proportional, and Predictable

By **Andrea Dugo** *(Economist),* **Fredrik Erixon** *(Director) and* **Dyuti Pandya** *(Analyst)*

EXECUTIVE SUMMARY

The Digital Markets Act (DMA) marked a major shift in EU competition and regulatory policy, moving from an effects-based and ex-post approach to a prescriptive, ex-ante regulatory framework. While the DMA rested on some clear observations about competition in platforms markets, the Act also came with some conceptual ambiguities and structural flaws. They could have been addressed in the implementation and enforcement of the DMA but, unfortunately, these processes have exacerbated rather than moderated the problems. In this Policy Brief, we argue that there is now a new opportunity to improve enforcement practices and make the DMA more pragmatic, proportional, and predictable.

The central argument is that there is a growing gap between the DMA's stated goals, its enforcement, and real-world effects. While some targeted interventions in the DMA implementation improved competition and specific user experiences somewhat, it is difficult to find any evidence supporting the proposition that the DMA has meaningfully reshaped competitive dynamics in digital markets. However, business compliance costs have increased significantly – and, importantly, not just for so-called gatekeepers. DMA enforcement is now also generating tensions with other EU regulatory frameworks, particularly in the areas of data protection, cybersecurity, intellectual property rights, and consumer protection.

A key concern is that enforcement has gradually expanded the DMA beyond its original scope. Enforcement actions and regulatory discussions now seem to extend into areas such as cloud computing and generative AI, often without clear evidence that these sectors exhibit the same structural competition problems that motivated the DMA. Perhaps the expansion is motivated, perhaps it is not. It is difficult to make a judgement when the European Commission do not present material evidence supporting their enforcement actions. The risk is that expansion weakens the coherence and legitimacy of the framework in the absence of transparent analysis and robust evidentiary standards.

DMA enforcement also presents structural challenges. Its reliance on predefined obligations and broad legal concepts – such as "gatekeeper" status or "interoperability" – grants significant discretion to regulators while limiting the role of effects-based analysis. In practice, this has led to increasing regulatory uncertainty and, increasingly, a shift from regulating conduct to influencing product design, pricing structures, and platform architecture.

Enforcement dynamics further complicate the picture. Parallel investigations by national authorities, combined with overlapping EU legal frameworks, have created a layered system of governance in which the same conduct may be assessed under multiple regimes. This risks duplication, inconsistent outcomes, and fragmentation of the Single Market – precisely the outcomes that the DMA was intended to prevent.

The enforcement of interoperability obligations illustrates these tensions particularly clearly. Originally conceived as a tool to lower entry barriers, interoperability is increasingly applied as a prescriptive design requirement, often without sufficient regard for differences across platforms or for legitimate concerns related to privacy and security. In some cases, these obligations may even weaken existing competitive dynamics, while introducing new technical and regulatory risks.

More broadly, the DMA increasingly reflects a shift in EU regulatory philosophy, from prohibiting harmful conduct to prescribing how digital systems should operate. When combined with other prescriptive regimes, this approach creates unavoidable trade-offs between competition, security, and privacy objectives.

This Policy Brief argues that better enforcement approaches could improve the DMA's chances of achieving its objectives. Enhancing enforcement approaches require a recalibration of methods and instruments towards greater predictability, better proportionality, and more evidence-based decision-making.

To this end, five key recommendations are proposed:

- Clarify the DMA's core objectives to prevent enforcement drift.
- Strengthen evidentiary standards for enforcement actions.
- Apply interoperability obligations in a proportionate and context-sensitive manner.
- Improve coordination with adjacent regulatory frameworks.
- Ensure that any enforcement expansion is grounded in clear competition-based evidence.

In sum, for the DMA to improve competition and user experience – and not damage them and Europe's security and digital capabilities – it needs better enforcement and alignment with the original purpose of supporting competitive, innovative, and user-oriented digital markets.

1. INTRODUCTION

The debate about the Digital Markets Act (DMA) has often been in binary terms – whether the regulation is "good" or "bad" or if one is "for" or "against". However, this framing is increasingly unhelpful. While the DMA started with some conceptual ambiguities and structural flaws, it was always understood that the actual enforcement of the DMA could make the regulation clearer and fit for its purpose of promoting competitive and innovative platform markets. Attention should therefore shift towards how it operates in practice and the challenges arising from its implementation and enforcement, including the integration of the DMA with competition policy and other key EU regulations in areas such as cyber security and data integrity.

There is a strong case for improving DMA enforcement. In the first place, enforcement has developed in ways that err on the wrong side of the original DMA design. In short, the DMA has partly developed to become something that legislators never intended. For instance, the regulator is now using enforcement and specification proceedings for regulatory purposes of product design and price. Moreover, the Act now routinely challenges other EU regulation on data privacy and cybersecurity, and the European Commission seems to have settled on an administrative hierarchy that puts the DMA at the top.[1] When the DMA does not cohere with other EU regulations, it seems that the DMA should have highest priority. This was not the intention with the DMA.

Moreover, key concepts within the DMA are being re-interpreted, if not redefined. This is especially the case with many enforcement measures aiming at interoperability – mandating platforms to provide open and equal access for all third parties regardless the effects on architecture, safety, business model, and the actual outcomes for competition and consumers. In the first process of DMA implementation, the Commission focused on some obvious and "legacy"-oriented aspects of interoperability – often reflecting some past or current antitrust cases. Since then, however, demands are raised that just cannot be met by platforms without reducing using service quality, safety, and a reasoned view of system integrity. Rather, the enforcement on interoperability now gives the impression of DMA regulators chasing some platform competition ghosts from the 2010s – or fixing the market as it looked like then.

The case for improving DMA enforcement is also reinforced by the Acts gradual expansion. Some of these expansions reflect the dynamic character of markets, technology, and competition. For instance, three investigations into cloud services have recently been opened by the European Commission, despite these services not having been classified as Core Platform Services – let alone fulfilling conditions for such designation. Moreover, there is general talk about including Large Language Models into the scope of DMA enforcement: indeed, a new specification proceeding is also taking aim of such an AI tool.

Perhaps the expansions are motivated, perhaps they are not. The issue is not necessarily one about the exact market and product boundaries of the DMA but more about the material bases that motivate enforcement actions. Under the DMA, enforcement can work on very flexible terms

[1] See Dugo, A. and Erixon, F. (2026, April 13), When Rules Collide – Regulatory Frictions Around the DMA and the Future of the EU's Digital Framework. ECIPE Insight. Available at: https://ecipe.org/insights/regulatory-frictions-around-dma/

with little regard for material motivations and outcomes. For instance, actions can be mandated that only have the impact of redistributing market power: while an enforcement action reduces the serviceability of one gatekeeper, it empowers another gatekeeper or a large company with an even stronger power in the end market or, say, over SMEs. Now the evidence requirements in actual enforcement are low, and before the DMA is expanded there is a great need to establish better protocols for what evidence and outcomes that motivate enforcement action.

The review of the DMA has been a good opportunity to reflect on the past and the future enforcement of the DMA. So far, however, the review has not included much more than a public consultation that, predictably, became a shouting match between different stakeholders. No economic impact assessment or review study has been published. To date, only two Commission-led reports on the DMA exist, and these provide very limited insight into its effects on competition, focusing largely on compliance rather than outcomes. As DMA enforcement continues to expand, there should be a desire to evaluate actual effects and discuss how it best could be enforced to support its objectives. Given all the ink, money, and time that has already been spent on the DMA, it should be in the public interest to make sure that adequate efforts are done to improve its operation. This is standard duty of care.

After all, the experience of many from the first years of the regulation suggests a gap between the DMA's stated motivations and its practical outcomes – especially measured as real market developments. Thierry Breton, Europe's former Digital Commissioner and principal political advocate of the DMA, branded it as a regulation to "reorganise the digital space".[2] By that score, the DMA must be seen as a failure. While platform markets have changed profoundly through innovation and technological change, it just is not the case that the DMA has changed market outcomes. In fact, it is implausible it ever could.

Taken together, some user experiences have improved, and others have been impaired because of DMA actions; most actions have not had any material consequence at all on competition. However, business compliance costs have gone up remarkably and will likely continue to do so as DMA enforcement increasingly conflicts with EU regulations on cybersecurity and privacy, and thereby exacerbates liability exposure. While some design flaws in the DMA could ideally be improved, it is more important to focus on making enforcement better fit for purpose.

In this Policy Brief we will discuss the developments of the DMA and propose ways to improve its enforcement. It proposes five key improvements to make DMA enforcement more predictable, proportional, and pragmatic. The Policy Brief starts with a review of the DMA and how it has evolved since its inception (Chapter 2). It then discusses the enforcement of the DMA and how the approach has caused problems (Chapter 3), before offering concrete recommendations aimed at improving enforcement and ensuring more coherent coexistence with other regulations (Chapter 4).

[2] Breton, T. (2021, March 25). DSA/DMA Myths – What is the EU digital regulation really about? LinkedIn Post. Available at: https://www.linkedin.com/pulse/dsadma-myths-what-eu-digital-regulation-really-thierry-breton/

2. THE DMA AND ITS EVOLUTION

The DMA is premised on a regulatory preference for speed: to "fix" platform competition problems before they have been established, it is relying on predefined one-size-fits-all obligations rather than case-specific assessments or sector-specific competition law regimes. By this design, the EU aimed to address competition concerns such as those arising from vertical restraints. While such restraints are not new, the evolution of digital platforms in the 2010s exacerbated some of them through their network effects.

However, a conceptual problem right at the centre of the DMA is that network effects often arise because they deliver real gains for users. For instance, network effects emerging through the simplicity in managing different services in one integrated platform with high standards for consumer safety and usefulness are obvious. Hence, the distinction between legitimate competitive advantage and consumer choice, on the one hand, and concerns related to what the DMA considers to be platform market-power abuse, on the other, is often blurred.

Such complexities have traditionally warranted a rule of reason approach, as reflected in EU competition law, which rely on effects-based assessment. Historical developments point even more in this direction. The 1999 modernisation of EU competition law, for instance, was a decisive shift away from rigid, formalistic rules towards a more economic, effects-based analysis. Rather than imposing blanket prohibitions, the framework allowed for the assessment of efficiencies and introduced market share thresholds, requiring firms to justify potentially restrictive practices.[3]

More importantly, this reform marked a broader shift towards ex-post enforcement. It was based on the recognition that increasing contractual and market complexity limited the effectiveness of centralised regulatory fine-tuning. Instead, enforcement was complemented, and in part replaced, by mechanisms that decentralised assessment to national authorities, courts, and sometimes to firms themselves through self-assessment.

The complexity and evolving nature of digital markets would seem to reflect the principles behind the modernisation of competition policy. While the DMA took a different orientation – partly for clear reasons – the reality is that market and technological complexity has continued to grow. This raises questions as to how pre-emptive regulatory obligations can be appropriately calibrated – and under what administrative conditions? Clearly, part of the answer depends on what actions that are taken and what empirical and legal grounding that are motivating them.[4] In essence, the principal conflict between rigid pre-emptive rules and an evolving technological market points to the need for enforcement that is both adaptive, attentive to market competition, and observant of outcomes.

---

[3] Boscheck, R. (2000). EU policy reform on vertical restraints: An economic perspective. World Competition: Law & Economics Review, 23(4), 3–49 as referenced in Boscheck, R. (2024). The EU's Digital Markets Act: Regulatory reform, relapse or reversal? Intereconomics: Review of European Economic Policy, 59(3), 154–159.

[4] Boscheck, R. (2023). Digital markets act: Regulatory reform, relapse or reversal? Concurrences Review. Available at: https://awards.concurrences.com/IMG/pdf/lpab066.pdf

Other developments point in the same direction. The evolution of DMA enforcement means that it increasingly sits closer to other EU regulations. Anticompetitive conduct in DMA and adjacent markets has long been recognised, and were and are being addressed under established competition law. Prior to the DMAs adoption, the EU regulatory framework already included instruments addressing similar concerns.[5] The Platform-to-Business (P2B) Regulation of 2019,[6] for instance, sought to enhance transparency in the relationship between platforms and business users. Likewise, the Unfair Commercial Practices Directive emphasised fairness and established a "blacklist" of prohibited practices.[7] The contestability objective of the DMA reflects broader regulatory concerns that extend beyond competition law, including objectives akin to media pluralism pursued under the Audiovisual Media Services Directive.[8]

More importantly, the DMA enforcement on data use and processing, data portability and user consent intersect with the framework established by the General Data Protection Regulation (GDPR).[9] While much of the overlap arises in relation to the GDPR, there also appears to be increasing interaction with the other data instruments such as the Data Act and the ePrivacy Directive. Although formally distinct, these frameworks increasingly converge in regulating the use of data and related digital infrastructures, including cybersecurity concerns addressed by the Cybersecurity Resilience Act and the NIS2 Directive.[10] [11] As the EU seeks to sharpen cybersecurity rules and mandates much more cybersecurity control on all companies, the coherence between different regulations obviously becomes more important.

However, the DMA's initial reliance on presumptions and the more aggressive enforcement method increasingly creates tensions in the EU regulatory framework. While these presumptions appear sufficient to enable the Commission to initiate enforcement measures and proceedings, they are certainly causing problems when enforcement is not attentive of other regulations and what they seek to achieve. When presumptions are used in a programmatic way they can also steer enforcement away from practical ways to learn if a regulation works as intended, how markets are changing – and, of course, how it interacts with other regulations.

Even resourceful gatekeepers are often in a quandary when confronted by these programmatic presumptions in enforcement demands from DMA regulators. They are often divorced from

---

5 Bostoen, F. (2023). Understanding the digital markets act. The Antitrust Bulletin, 68(2), 263-306.

6 Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57 (hereafter: P2B Regulation).

7 Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-toconsumer commercial practices in the internal market [2005] OJ L149/22.

8 Directive 2010/13/EU of the European Parliament and of the Council on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2010] OJ L95/1, as amended by Directive (EU) 2018/1808 of the European Parliament and of the Council amending the Audiovisual Media Services Directive in view of changing market realities [2018] OJ L303/69.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (hereafter: GDPR).

10 See: Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data, OJ L, 22.12.2023. (hereafter: Data Act); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), OJ L 201, 31.7.2002. (hereafter ePrivacy Directive); Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L, 2024 (Hereafter Cyber Resilience Act); Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive), OJ L 333, 27.12.2022, pp. 80–152 (Hereafter NIS2 Directive).

11 Bostoen, F. (2023). Understanding the digital markets act. The Antitrust Bulletin, 68(2), 263-306

actual product and market reality. For instance, gatekeepers have been confronted by demands that, in a generous analysis, have negligible impacts on competition and markets. However, they are causing significant business costs and uncertainty about whether a service can actually be supplied in the EU market. In other cases, companies are faced by enforcement demands that presume a control of third parties and other companies in the value chain they do not have, or that put their systems for protecting trust and reputation, privacy and cybersecurity at risk.

Strangely, the enforcement approach has made the DMA both overly rigid and excessively open ended. Presumptions make DMA enforcement programmatic and insensitive to real product and market developments and concerns. At the same time, it allows for a change in regulatory scope that is very flexible and enables a presumption-based application in places that were never included in the original design. In this complex environment, it is difficult to find out how decisions are made, who make them, and on what grounds. The DMA seeks to encourage contestability, but those who enforce the regulation seem reluctant to present findings, evidence, and motivations that make their decisions understandable, let alone contestable.

There is now an opportunity to change the enforcement approach. The risk of mission creep was known at the time when the DMA was conceived. The DMA incorporates a built-in review mechanism, requiring the Commission to assess the functioning of the Regulation by 3 May 2026 and every three years thereafter. This review is intended to evaluate whether the rules are effectively contributing to the objective of ensuring fair and contestable markets, as well as their impact on business users, and to determine whether additional measures may be necessary to ensure the regulation's effectiveness.

Moreover, there is an opportunity to use the DMA review as a real learning mechanism that incorporates a culture of evaluation that helps everyone to better understand what has worked and what has not. This approach does not prejudice changes to the DMA – neither in scope nor in methods of application. However, it would help to make DMA enforcement fit for purpose.

3. FROM POLICY DESIGN TO REAL-LIFE ENFORCEMENT

The expansion of the DMA's scope and interpretative reach has begun to expose deeper structural tensions within the EU regulatory framework. As enforcement extends into new domains, business models, and practices, it increasingly operates as a form of *lex specialis*, effectively superseding or reshaping the application of existing legal regimes, including competition law and sector-specific rules.

The enforcement of a regulation is usually neglected in the literature but matters crucially for the outcomes of a regulation. Obviously, the actual text in the regulation is important. But the way a government or public entity operationalises and enforces a regulation equally impacts on the results and, ultimately, is what matters to those exposed to a regulation. This is especially the case in emerging and developing sectors: the competitive advantages of one company can rise rapidly, but new technology and innovation changes both the form and matter of competition. A strong market position – even market dominance – are in such examples fleeting concepts. It

requires an enforcement attitude that is observant of change and that do not take a command-structured approach.

And here there is room for improvement in how the DMA is enforced and how it impacts on parallel regulatory processes. In this chapter, we will go into some of the fundamental enforcement problems that have arisen.

3.1 Parallel National Enforcement and Gold-Plating

The *lex specialis* status of the DMA seems to be more observed in relation to other EU rules than to Member State applications of regulations. National competition authorities (NCAs) have initiated parallel or overlapping investigations into conduct that is already addressed by DMA enforcement. Obviously, duplicative compliance burdens increase legal uncertainty and sit awkwardly with rule-of-law principles. A company should not be punished twice for the same behaviour: at both the national and the EU level. Nor should it be regulated for the same behaviour by multiple actors – especially in a regulation (the DMA) that purports to harmonise European policy.

The reality is different. In several instances, national proceedings have targeted the same services and practices that fall within the scope of the DMA. This raises concerns about Member States effectively layering additional regulatory constraints on top of the core framework.[12] A prominent example is the action taken by the Bundeskartellamt against Amazon under Section 19a(2) of the German Competition Act (GWB). The case focuses on features of Amazon's marketplace, including systems designed to prevent the prominent display of unusually high or uncompetitive offers in the Featured Offer (Buy Box). Similar practices have also been subject to scrutiny at the EU level, notably in the Commission's earlier antitrust investigation and the commitments accepted from Amazon in 2022, and fall within the broader concerns addressed by the DMA under Article 5(3).[13]

Building on these types of overlap, the institutional framework of the DMA further reinforces a layered enforcement structure. While the Commission remains the sole enforcer of the DMA, national competition authorities are granted significant supporting competences to assist in its enforcement. This has led several Member States, both before and after the DMA became applicable, to adapt their domestic frameworks: some have introduced legislative amendments, while others have strengthened existing enforcement mechanisms and institutional cooperation. In Germany, for instance, Section 19a of the Act Against Restraints of Competition (ARC) was introduced to address the risks of market concentration arising from network effects. Although it was adopted shortly before the DMA came into force, the German "gatekeeper" regime goes beyond the DMA's scope: it is not limited to core platform services and enables the Federal Cartel Office (FCO) to intervene even in markets where a firm is not dominant.

---

[12] Chamber of Progress response to the first review of the Digital Markets Act; see: Italy AGCM A552 - Google's Data Portability (concluded July 2023); Germany BKA - Google Data Combination (concluded October 2023); Germany BKA - Google Automotive services and Maps (concluded April 2025).

[13] Amazon response to the first review of the Digital Markets Act.

Such developments do not rhyme with Article 1(5) DMA, which seeks to prevent Member States from imposing additional obligations pursuing the same objectives. By enabling national authorities to investigate or intervene in areas closely aligned with the DMA, these measures risk undermining the regulation's harmonising function, creating parallel enforcement pathways and potentially allowing NCAs to extend their role beyond that envisaged under the DMA.

On the one hand, the DMA expressly preserves the powers of NCAs to apply national competition and consumer protection laws. On the other hand, it centralises the enforcement of its own obligations in the Commission, while requiring NCAs to support that enforcement through investigative and information-sharing roles. The result is not a clear-cut separation, but rather a layered system of governance in which the same conduct by a gatekeeper may be enforced under multiple legal frameworks: the DMA's ex ante obligations, competition law's effects-based analysis, national digital regulation, and national consumer or commercial fairness rules. This gives rise to a form of functional concurrency: distinct legal regimes formally separate yet are substantively interconnected in parallel.

We saw this already with the Italian Competition Authority (AGCM) action against Google, where consumer protection law was used to address a consent mechanism involving the combination and cross-use of personal data without valid user consent,[14] conduct that also falls within the scope of Article 5(2) of the DMA. In response, Google committed to modifying its consent requests, including by introducing clearer information, improved customisation options, and explicit references to Article 5(2) DMA.[15]

A similar approach can be observed in proceedings involving Meta where the AGCM examined changes to terms and conditions in light of competition concerns, drawing on reasoning analogous to the Android Auto case.[16] In particular, the authority suggested that certain changes could amount to a denial of access to digital infrastructure for third-party undertakings, an issue that also overlaps with Article 6(6) DMA.

Another example can be found in the investigation launched by Spain's National Commission on Markets and Competition (CNMC) in which it alleged that Apple imposed restrictive conditions on developers distributing applications through the App Store. The practices under investigation, particularly limitations preventing developers from informing users about alternative offers, correspond to conduct already enforced under Article 6(4) DMA. In this context, the Commission had already initiated non-compliance proceedings against Apple in which it identified similar

---

[14] PS12714 - The Italian Competition Authority secures informed and freely given user consent to Google's linking of services; also see: Meyring, B., Reyntjens, T., Foon, S., and Leslie, W. (2025, December 9). Harmonised in Theory, Fragmented in Practice? The DMA Meets National Enforcement. Kluwer Competition Law Blog. Available at: https://legalblogs.wolterskluwer.com/competition-blog/harmonised-in-theory-fragmented-in-practice-the-dma-meets-national-enforcement/

[15] Ibid

[16] A576 - The Italian Competition Authority launches investigation into Meta over abuse of dominant position; also see: Martinez, R. A., (2025, December 1). The Roman Holiday of Denial of Access and the DMA's Centralised Enforcement System. Kluwer Competition Law Blog. Available at: https://legalblogs.wolterskluwer.com/competition-blog/the-roman-holiday-of-denial-of-access-and-the-dmas-centralised-enforcement-system/

concerns regarding Article 5(4) DMA and Article 6(4) DMA. These concerns relate in particular to restrictions on developers' ability to steer users towards alternative offers outside the App Store.[17]

These cases illustrate how NCAs can intervene in relation to conduct that is already covered by the DMA, even without directly applying it. While such interventions are formally grounded in a different legal basis, they are, in practice, replicating the enforcement of DMA-type obligations. There is a considerable degree of distortion of competition between member states already, and the rules of tackling unfairness in dependency relationships also diverge. Obviously, parallel enforcement should not happen under a harmonisation instrument designed to prevent fragmentation of the internal market. Therefore, national interventions risk creating divergent regulatory standards across Member States, undermining the uniform application of the rules. This, in turn, may result in a patchwork of obligations that varies by jurisdiction. In effect, it means the fragmentation of the Single Market – the very opposite of the "One Europe, One Market" concept that the EU rightly is advancing.

3.2 Enforcement and De Facto Design Regulation

The evolving enforcement of the DMA creates significant practical challenges for compliance. These concerns arise in relation to Article 6(11) of the DMA. This is reflected in the Commission's new proposed measures,[18] requiring Google to share search data, including query, click, and ranking information with third-party search engines and AI-based search services, including chatbots with search functionalities.[19] Search queries often contain highly sensitive personal information, and even when anonymised, such data carries a risk of re-identification when combined with other information.[20]

Google's current compliance efforts illustrate the difficulty of balancing these objectives. The company has made data available through tools such as Google Trends and introduced a European dataset licensing program covering billions of queries across 30 EEA countries. To address privacy concerns, it applies techniques such as frequency thresholding to remove low-volume queries that could reveal individual users. However, Google argues that such measures significantly reduce the utility of the data, particularly in smaller markets where meaningful insights often depend on low-frequency queries. This highlights a fundamental trade-off: stricter anonymisation enhances privacy protection but diminishes the competitive value of the data,

---

[17] Martinez, R.A., (2024, August 19). Between a Rock and a Hard Place: NCAs Trigger Antitrust Sanctioning Proceedings Against Gatekeeper Compliance Solutions. Available at: https://legalblogs.wolterskluwer.com/competition-blog/between-a-rock-and-a-hard-place-ncas-trigger-antitrust-sanctioning-proceedings-against-gatekeeper-compliance-solutions/?output=pdf

[18] European Commission. (2026, April 16). Commission proposes measures to Google on sharing search engine data with third parties under Digital Markets Act. Press Release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_825

[19] Similar remedies have also been considered in the US in antitrust proceedings against Google, reinforcing the growing regulatory focus on opening access to search data. McCabe, D. (2025, September 2). Google Avoids Harshest Penalties in Landmark Search Monopoly Ruling. New York Times. Available at: https://www.nytimes.com/2025/09/02/technology/google-search-antitrust-decision.html; While this does not amount to a formal break-up, it resembles a form of functional or quasi-structural separation, as it compels Google to grant competitors access to a core input of its search business. Search queries often contain highly sensitive personal information, and even when anonymised, such data carries a risk of re-identification. As a result, the DMA may inadvertently weaken data protection standards in its effort to enable competition.

[20] Barczentweicz, M. (2024, May 7). Google Previews the Coming Tussle Between GDPR and DMA Article 6(11). Truth on the Market. Available at: https://truthonthemarket.com/2024/05/07/google-previews-the-coming-tussle-between-gdpr-and-dma-article-611/

while increasing its utility for rivals may require weaker safeguards. The result is a structural dilemma at the heart of the DMA, which appears to demand both high data utility and robust privacy protection, even though these objectives may be inherently incompatible in practice.

The new proposed measures in form of data sharing obligations depart from established norms governing data access. And typically when data is shared, the scope of sharing is defined and tied to user consent obtained at the point of collection. By contrast, the approach under the DMA raises questions as to whether the users understand or control how their data may be further disseminated to third parties. In a regulatory environment otherwise characterised by increasing restrictions on data sharing and monetisation, mandating broad access to search data with limited user control appears difficult to reconcile with prevailing data protection principles.[21]

The evolving enforcement of the DMA creates significant practical challenges for compliance. Firms are required to continuously adapt their systems to meet shifting expectations, often at considerable cost. For example, Apple announced extensive changes to iOS, Safari, and the App Store to comply with the DMA, including the introduction of hundreds of new APIs, expanded app analytics for alternative browser engines, and new options for app distribution and payment processing.[22] These changes reflect a broader shift in Apple's ecosystem. Its operating system (OS) has traditionally been characterised by a relatively tightly controlled architecture, justified on grounds of security and user protection. The DMA, by contrast, challenges this model by requiring Apple to open aspects of its system for third parties to have equal access. As a result, Apple has had to redesign parts of its OS to accommodate requirements for which it was not originally intended.

The question that arises for DMA enforcers is how far interoperability obligations could be taken without jeopardising privacy and security – or be practically feasible? In the 2025 specification proceedings with Apple, the Commission made a legal argument on interoperability which, in effect, takes a maximalist view on interoperability obligations but a minimalist approach to privacy and security.

As part of its DMA implementation, Apple had already made substantive changes allowing for new sideloading and established a processes and resources for interoperability requests, including an appeal board with independent experts. The Commission went further and issued specific guidance that is detailed and prescriptive for third-party connected devices. It dismissed the security concerns raised by Apple and rather took a minimalist view of what security measures that are legitimate to protect the ecosystem. Even in situations where there are less trustworthy third-party operators requestion access, Apple cannot deny access.

---

[21] Saladrigas, F. C., Marmor, R., Kully, C. D., and Kocse, M. R. (2025, April 15). Google Search: Data Sharing as a Risk or Remedy? Holland and Knight LLP Cybersecurity and Privacy Blog Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=9045429c-04b2-43b0-b8c4-0c2bd9c8cc9d

[22] Apple. (2024). Apple announces changes to iOS, Safari, and the App Store in the European Union. Available at: https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

This view of protecting the integrity of the ecosystem features in the specification proceedings with Google. Like Apple, there is a protocol established for interoperability requests in Android, but what makes the case an indication of the more aggressive DMA enforcement attitude is that Android is open source. There is already full interoperability from the perspective of the source developer. While the Commission argues there are some limits to interoperability which reduced access only to apps preinstalled by the original equipment manufacturer (OEM), those OEMs are not the same as the source developer – they are different companies. Like the Apple cases, the additional interoperability indicated for Android can only be achieved by changes to basic architecture – and there is a trade-off in such changes: programmatic interoperability going beyond established protocols for the architecture can only be achieved by reducing integrity.

Beyond compliance costs, the nature of operating system enforcement obligations under the DMA raises deeper concerns. These obligations increasingly operate through product design requirements, moving enforcement away from traditional ex post competition law toward de facto design regulation. Questions such as how to structure user choice mechanisms illustrate this shift, as regulatory intervention begins to dictate interface-level decisions.

These tensions are already visible under Article 5(4). For instance, Google has been required to allow developers to include links within Play Store applications directing users to external offers, including alternative payment systems. Google's proposed compliance mechanism, the External Offers Program (EOP), highlights the difficulty of reconciling such obligations with cybersecurity concerns,[23] particularly given Android's open architecture and reliance on platform-level safeguards.

Apple has faced similar pressures. Anti-steering and alternative payment provisions constrain its ability to differentiate between native and external payment systems on the basis of security and privacy disclosures, as such differentiation may be interpreted as discouraging user choice. While implementation has introduced some flexibility, the underlying presumption in favour of openness risks weakening established protections in payment security and user data handling.

This raises a broader question: what market outcomes are DMA enforcement actions intended to achieve? To date, these measures appear to reflect programmatic enforcement of regulatory presumptions such as the belief that increased openness necessarily enhances competition, rather than interventions clearly tied to demonstrable improvements in contestability or consumer welfare.

Rather than reducing market power, such measures may instead contribute to its redistribution. This has been the outcome of other DMA-mandated changes. For instance, changes introduced by Google under Article 6(5), particularly in the display of flight search results, appear to increase the visibility of intermediaries such as online travel agencies, which may in turn displace airlines in search rankings. Platforms such as Kayak often display offers mediated by online travel

[23] Google. (2025). Enrolling in the external offers programme. Available at: https://support.google.com/googleplay/androiddeveloper/answer/14372887

agencies, which often make it more difficult for consumers to distinguish between intermediary and direct airline offers.[24]

As a result, airlines are increasingly forced to rely more heavily on paid visibility or third-party platforms to reach consumers, effectively shifting market power rather than reducing it. Moreover, the increased prominence of intermediaries reduces transparency for users, who may not clearly distinguish between direct airline offers and those provided through third parties. At the same time, these intermediaries are not subject to the same regulatory obligations as airlines, potentially creating an uneven playing field.[25]

Further evidence of these effects can be observed in related markets, particularly in hotel search services. Design changes have also affected Google Hotel Ads. In 2024, click data from a period of just over three months following the implementation of DMA-related changes showed a reported 30 per cent decrease in traffic volume in EU markets subject to the Regulation. Consequently, the share of direct bookings reportedly fell to 36 per cent, increasing hotels' dependence on intermediaries and negatively affecting their profitability.[26] These developments are linked to changes in how Google presents travel search results in order to comply with the DMA. Users no longer have access to certain previously integrated functionalities, such as viewing calendar-based price comparisons, accessing elements of the Google travel interface, or directly navigating via Google Maps links to hotel locations.

Such enforcement effects were not part of the DMA's original conception as a tool to address market power. In fact, the Commission's Impact Assessment said such market effects (reduced usefulness for business users) would not occur. Instead, they illustrate how its application is extending into areas that directly affect business models and product architecture, reinforcing concerns that the regulation is evolving beyond its initially defined scope.

What the enforcement approach does, in effect, is to shift the regulatory focus from whether access must be granted to how that access should be implemented in practice. This shift has important consequences. Once access is no longer conditioned on integrity, regulators are required to determine the scope, quality, and modalities of access, thereby drawing them into specifying technical interfaces, system architectures, and even user-facing functionalities. In digital environments, where system behaviour is shaped by technical architecture, such specification amounts in practice to direct intervention in product design.[27]

---

[24] A4E. (2024). A4e's Position Paper On The Implementation Of The Dma And Alphabet's Compliance With Its Obligations. Available at: https://a4e.eu/wp-content/uploads/A4E-position-on-the-DMA-implementation.pdf

[25] Ibid

[26] Delgado, J. (2024, May 6). The DMA enforcement has caused a 30% drop in clicks and bookings on Google Hotel Ads. Mirai. Available at: https://es.mirai.com/es/blog/la-aplicacion-de-la-dma-hunde-un-30-clics-y-reservas-en-google-hotel-ads/?utm_source; further examples of these changes will be discussed in a forthcoming paper (April 2026) examining the economic impact of the DMA.

[27] Erixon, F. and Pandya, D. (2026). The DMA Is Not Fixing Competition, It's Redesigning It. ECIPE Insight. Available at: https://ecipe.org/insights/dma-redesigning-competition/

3.3 Interoperability Conflicts with Privacy, Security, and Intellectual Property Regulation

The implementation of DMA measures is also becoming more complex, reflecting a changing direction in the way the Commission enforces the regulation. This is particularly the case as mandated actions under the DMA increasingly intersect with other EU frameworks, raising questions not only about compliance with the letter of the law, but also with its underlying objectives. A central tension emerges where the DMA's pro-openness logic – particularly obligations to open platforms and facilitate data access – collides with safeguards embedded in the GDPR, especially with regard to the processing of sensitive personal data and system-level ambitions to improve cybersecurity and frictions with intellectual property protection.

For this reason, it is worth delving a bit deeper into the way DMA enforcement measures have conceptualised interoperability, because the level of complexity in enforcement decisions gives the impression that the DMA has been changed. Interestingly, the Commission's original proposal for the DMA contained certain interoperability-related obligations, primarily within Article 6. These provisions were less detailed and often subject to further specification through regulatory dialogue. During the legislative process, these obligations were significantly elaborated and made more concrete, resulting in highly detailed provisions. At the same time, the co-legislators introduced a new and structurally distinct interoperability regime in Article 7, specifically addressing interoperability for interpersonal communication services.

However, the logic of interoperability under Article 7 does not translate straightforwardly across different types of digital services. While it is designed to address network effects in messaging services, its extension to other contexts raises important limitations. For instance, unlike messaging services, social networking services (SNS) rely heavily on content curation and algorithmic recommendation systems. User experience is shaped not only by connectivity, but by platform-specific ranking, visibility, and recommendation mechanisms, which complicate the very notion of interoperability. As a result, interoperability in such contexts is unlikely to replicate meaningful competitive conditions. Instead, it may provide gatekeepers with subtle and difficult-to-detect ways to limit the effectiveness of interoperability, for example through ranking or visibility adjustments.

Moreover, there is limited empirical evidence that interoperability opportunities are widely used in practice. Although the DMA allows third-party providers to request interoperability with designated gatekeepers, there is little indication that a significant number of smaller services have successfully integrated with major platforms. In some cases, providers have actively declined to pursue interoperability. For example, Signal has indicated that it is unlikely to engage in such arrangements, citing concerns related to user privacy and its organisational model.[28] These observations suggest that interoperability is not only a technical or regulatory issue, but also depends on the strategic incentives of firms. As a result, DMA enforcement tends to overestimate both the demand for and the feasibility of interoperability as a tool for promoting competition.

[28] Euroconsumers response to the first review of the Digital Markets Act.

However, the more far-reaching concerns arise in relation to Article 6(7), which operates at the level of system design and raises more direct conflicts with privacy, security, and other regulatory frameworks. This tension between DMA enforcement and the GDPR is first reflected in the joint publication by the European Commission and the European Data Protection Board (EDPB) on the interplay between the two regulations.[29] While the guidelines formally emphasise that both frameworks should be applied in a coherent and complementary manner, they introduce a clear operational bias: where multiple GDPR-compliant options exist, gatekeepers are expected to favour those that least undermine the objectives of the DMA. In practice, this amounts to a functional prioritisation of DMA compliance, even in the absence of a formal hierarchy between the two regimes.

In particular, the tendency is also reflected in the way the Draft Joint Guidelines address risk, as they appear to downplay the data protection and security concerns arising from DMA obligations. They tend to interpret the DMA's security and privacy provisions narrowly, for instance by limiting the ability of gatekeepers to warn users about potential risks associated with data portability, and by constraining their capacity to exclude high-risk or potentially harmful third parties as recipients of user data.[30] But the regulatory reality is far less straightforward. There are many situations in which no meaningful GDPR-compliant alternatives exist, or where authorities are effectively requiring firms to disregard data protection limitations in order to comply with data-sharing mandates. This is not merely theoretical. The specification proceedings and enforcement actions already illustrate how platforms are required to enable third-party access to user data while simultaneously remaining accountable for how that data is processed by external actors. [31]

This also helps explain the limited attention given in the guidelines to interoperability obligations under Article 6(7), despite their potentially significant implications for access to system-level functionalities and user data. This is particularly problematic given that, although the Commission has formally recognised that the implementation of Article 6(7) must comply with principles such as proportionality and applicable data protection rules,[32] its approach in specification decisions appears to constrain the safeguards that gatekeepers may invoke, notably by limiting them largely to integrity-related measures. Such an approach requires careful justification, as it risks sitting uneasily with Article 6(7) read in conjunction with Article 8(1) of the DMA.

The underlying conflict reflects foundational incompatibilities between different regulations. For instance, the GDPR is built around principles such as purpose limitation, data minimisation, and accountability. By contrast, the DMA requires broad, and in some cases continuous and real-time, access to data across services and business models. In practice, this can significantly expand the scope of data flows beyond what would typically be considered proportionate under GDPR

---

[29] European Commission & European Data Protection Board, Draft joint guidelines on the interplay between the Digital Markets Act and the General Data Protection Regulation (GDPR) for public consultation, 9 October 2025, Available at: https://digital-markets-act.ec.europa.eu/.

[30] Barczentewicz, M. (2025, December 4). ICLE Comments on the Interplay Between DMA and GDPR. ICLE Regulatory Comments. Available at: https://laweconcenter.org/resources/icle-comments-on-the-interplay-between-dma-and-gdpr/

[31] Dugo, A. and Erixon, F. (2026). When Rules Collide: Regulatory Frictions Around the DMA and the Future of the EU's Digital Framework. ECIPE Insight. Available at: https://ecipe.org/insights/regulatory-frictions-around-dma/

[32] European Commission. (2025, March 19). Decision pursuant to Article 8(2) of Regulation (EU) 2022/1925 (Case DMA.100204 – Article 6(7) – Apple iOS and iPadOS – SP – Process) (C(2025) 3001 final)

standards, leading to effects such as "consent fatigue", where users are confronted with repeated and complex permission requests that undermine meaningful control over their data.[33]

Concrete examples illustrate how these tensions materialise. Under the DMA, a user may request that a third-party app – such as a budgeting or fitness service – connects to their primary platform account. The platform is then required to facilitate access to potentially sensitive data, including transaction histories or location data. Yet, the same platform remains responsible under the GDPR for ensuring that such transfers comply with strict data protection requirements. They are also held liable for it. At the same time, its ability to screen or restrict third-party access based on security or privacy risks has proven to be limited by DMA enforcement. This creates a structural situation in which platforms must enable data sharing while bearing responsibility for risks they cannot fully control.[34]

For instance, Apple's Exposure Notifications framework, developed during the COVID-19 pandemic, allowed authorised applications to detect proximity between devices in order to notify users of potential exposure. Given the highly sensitive nature of such data, effectively creating a log of user encounters, Apple imposed strict limitations on access, including restricting the API to specific public health use cases and excluding even its own internal teams from broader use.[35] If interoperability obligations are applied without sufficient regard to context, this could require opening access to sensitive interfaces to a wide range of third-party services, including social networks or advertising platforms. In such scenarios, interoperability could enable the construction of detailed social graphs without meaningful user awareness or consent.

These principal tensions are also at the centre of enforcement cases covering app distribution and platform security. The DMA's requirements to allow alternative app distribution channels and reduce gatekeeper control constrain how platforms can rely on centralised vetting procedures. For example, there are cases where applications[36] disguised as benign services such as browsers or utility apps have provided access to illegal streaming content after installation, or functioned as "trojan horse" applications. Once installed, these applications may have access to user data through device permissions opening road to security breaches. More recently, the emergence of a pornographic application distributed outside traditional app store controls has been cited as an illustration of how reduced gatekeeper oversight may enable the circulation of content that would otherwise be subject to stricter review. While such risks are not new, the DMA increases the complexity of maintaining platform integrity by reducing the degree of security controls traditionally exercised by gatekeepers.

---

33 Barczentewicz, M. (2025, December 4). ICLE comments on the interplay between DMA and GDPR. International Center for Law & Economics. https://laweconcenter.org/resources/icle-comments-on-the-interplay-between-dma-and-gdpr/

34 Dugo, A. and Erixon, F. (2026). When Rules Collide: Regulatory Frictions Around the DMA and the Future of the EU's Digital Framework. ECIPE Insight. Available at: https://ecipe.org/insights/regulatory-frictions-around-dma/

35 Apple response to the first review of the Digital Markets Act.

36 Laporte, C. (2025, September 25). DMA : Apple explique pourquoi l'iPhone est privé de certaines nouveautés. MacGeneration. Available at: https://www.macg.co/aapl/2025/09/dma-pourquoi-les-iphone-et-airpods-sont-brides-en-europe-selon-apple-303933; Gurman, M. (2025, February 4). Apple Blasts EU Laws After First Porn App Comes to iPhones. Bloomberg. Available at: https://www.bloomberg.com/news/articles/2025-02-03/apple-blasts-eu-app-laws-after-first-porn-app-comes-to-iphones?utm_source=website&utm_medium=share&utm_campaign=copy&embedded-checkout=true

These practical risks illustrate broader concerns of enforcement coherence. Article 8(1) of the DMA, requires that its obligations be implemented in compliance with other applicable legal frameworks, including those governing cybersecurity, consumer protection, and product safety. While this provision appears to promote regulatory coherence, in practice it introduces a significant degree of ambiguity, as these regulations pursue different objectives and operate according to distinct legal logic. As a result, platforms face conflicting obligations: they are required to open their systems and facilitate access under the DMA, while simultaneously ensuring high levels of security and compliance under parallel regulatory regimes.

The mere inclusion of Article 8(1), which demands gatekeeper compliance with other laws (e.g., cybersecurity and product safety) does not resolve the underlying dilemma. So far, it has functioned primarily as a saving clause rather than a harmonising or guiding provision in actual enforcement. It requires compliance with other legal frameworks but does not provide clear guidance on how to reconcile potentially conflicting obligations. Security in digital ecosystems is often dependent on end-to-end control over hardware, software, and distribution channels. As platforms are required to open elements of their systems, their ability to prevent the introduction of unverified or potentially harmful applications is reduced. While safeguards such as post-installation checks and permission controls remain available, they may not fully replicate the level of oversight associated with more closed systems. Vulnerabilities may arise through less controlled distribution channels, as illustrated by past incidents involving malicious software exploiting weaker points of access.

Conflicts are particularly visible in the interaction between the DMA and the EU's broader cybersecurity framework. While these frameworks aim to strengthen system integrity, risk management, and resilience, the DMA requires platforms to prioritise openness and interoperability – even where this may weaken existing security safeguards. Interoperability mandates can significantly expand the "attack surface" of digital systems by introducing new technical entry points that were not originally designed for external access, increasing exposure to malware, spyware, and other forms of cyber intrusion. The Commission has so far dismissed concerns raised by gatekeepers that mandated interoperability and access obligations may increase vulnerabilities. However, firms are increasingly confronted with situations in which compliance with DMA obligations entails accepting heightened cybersecurity risks or limiting the effectiveness of protective measures.[37]

Recent enforcement practice illustrates how these constraints materialise in concrete cases. Business users have invoked Article 6(7) to request access to Apple's Just-In-Time (JIT) compiler in iOS, a core component underlying browser engine functionality. JIT compilation enables code to be dynamically generated and executed at runtime, which is essential for performance but also inherently sensitive from a security perspective. Granting third parties access to this functionality would require allowing the injection and execution of code within a highly privileged part of the operating system. This significantly expands the potential attack surface, as malicious or poorly secured code could exploit vulnerabilities at a system level rather than within a confined application environment. For this reason, JIT engines have historically been subject to strict

[37] Ibid.

platform-level controls and sandboxing restrictions. This helps explain why such proposals have been described by cybersecurity experts as creating a "major security vulnerability".[38]

This dynamic also introduces additional complexity in relation to intellectual property protection.[39] In practice, mandated interoperability may require gatekeepers to disclose interface specifications, technical documentation, or system functionalities that would otherwise be protected under copyright, trade secrets, or database rights. Similarly, data access and portability obligations can also extend to datasets that benefit from legal protection, raising questions about the limits of required sharing. The concern may become more pronounced where competitive dynamics are already contestable. In such circumstances, intervention may misdiagnose the source of competitive pressure and impose access obligations where they are not necessary.

While these tensions do not reflect a direct contradiction between the DMA and IP law, they nevertheless reflect a recalibration of the balance between the two regimes. The DMA seeks to shift this balance in favour of market contestability, potentially at the expense of IP protection. In particular, it risks undermining innovation incentives by compelling access to protected assets irrespective of whether those rights have been exercised abusively. Moreover, emerging tensions between gatekeepers themselves further illustrate the complexity of the issue.

This marks a departure from established EU competition law, where compulsory access to IP has been confined to exceptional circumstances, requiring a showing of indispensability, the elimination of effective competition, and, in some cases, the prevention of a new product. Under settled case law of the Court of Justice of the European Union, notably *IMS Health* and *Magill*, a refusal to license an IP right constitutes an abuse under Article 102 TFEU only in such exceptional circumstances. This typically requires that the refusal is liable to eliminate effective competition, lacks objective justification, and prevents the emergence of a new product for which there is potential consumer demand. By contrast, the DMA imposes ex ante regulatory obligations that depart from traditional ex post antitrust liability and do not require compliance with these stringent, case-specific conditions, thereby lowering the threshold for overriding IP exclusivity.

4. MAKING THE DMA MORE PREDICTABLE, PROPORTIONAL, AND PRAGMATIC

Digital markets are evolving rapidly, particularly with developments in AI and new digital ecosystems. These technological shifts are likely to reshape competitive dynamics far more quickly than regulatory DMA enforcement ever can. Against this backdrop, the actual enforcement of the DMA can be substantially improved by making the whole DMA universe less programmatic and more proportional, pragmatic, and predictable. Especially, it needs to be built on evidence-based measures.

---

[38] Kohlenberger, J. (2025, September 5). When interoperability mandates weaken security—JIT happens. Trusted Future. https://trustedfuture.org/when-interoperability-mandates-weaken-securityjit-happens as referenced in Manne, G. A., Auer, D., Radić, L., Ünekbaş, S., & Zúñiga, M. A. (2025). ICLE Response to First Review of the Digital Markets Act. Available at: https://laweconcenter.org/resources/icle-response-to-first-review-of-the-digital-markets-act/

[39] Streel, D. A., and Monti. G (2026). DMA regulatory interplays. CERRE Issue Paper. Available at: https://cerre.eu/wp-content/uploads/2026/02/CERRE_DMA-Regulatory-Interplays.pdf

The scope of the DMA should of course be adapted to new market and technological circumstances: a static regulation that cannot expand in scope is not principally useful. But adaptations and expansion cannot just be a one-way ticket for more enforcement and a style of enforcement that is intimidating but ineffective. If the DMA should be future-proofed and made relevant for the world of technology in the late 2020s, it cannot remain stuck in platform market concerns of the 2010s. The best way forward is rather to integrate the DMA with the norms and standards of general competition policy, and radically increase the coherence with other key EU regulations.

Five key policy recommendations follow from this analysis. They all focus on the enforcement of the DMA and points to a greater role for the European Commission to develop a more coherent application of the DMA in relation to other laws and a more evidence-based approach that ensures that a regulation has a desirable effect without jeopardising other EU objectives. Importantly, these recommendations are not just about the enforcement approach by the single unit that administrates that DMA. A clear priority is to engage other parts of the European Commission that manage other regulations.

1. **The European Commission should clarify the regulatory objectives guiding enforcement,** ensuring that the DMA remains anchored in its original competition-focused rationale and does not drift towards broader, undefined objectives and policy goals.

2. **DMA regulators should establish clearer and more consistent evidentiary standards,** particularly in relation to key concepts such as self-preferencing and interoperability, to limit discretionary and uneven enforcement.

3. **The interoperability obligations should be applied in a proportionate and context-sensitive manner,** taking into account legitimate considerations such as security, system integrity, and user protection, rather than imposing uniform design requirements.

4. **The European Commission should strengthen coordination with adjacent regulatory frameworks,** including the GDPR, cybersecurity rules, and relevant international standards such as those developed by the International Competition Network, in order to avoid conflicting obligations and ensure regulatory coherence.

5. **Enforcement of the DMA to emerging and rapidly evolving sectors and services such as cloud services and generative AI must be substantiated by evidence that is connected to competition concerns.** Expanding enforcement into new areas risks imposing obligations that are not calibrated to evolving technological and market realities. A more cautious, evidence-based approach would allow for clearer assessment of competitive dynamics before introducing ex ante obligations.