esade
RAMON LLULL UNIVERSITY

EsadeGeo-Center
for Global Economy
and Geopolitics

Implementing the Digital Markets Act

Policy Recommendations for Competitive, Innovative and Trusted Digital Ecosystems

JUNE 2026

Do Good.
Do Better.

esade
RAMON LLULL UNIVERSITY

EsadeGeo-Center
for Global Economy
and Geopolitics

AUTHORS

Mara Balestrini
Senior Fellow, EsadeGeo

Laia Serrano i Sorroca
Research Assistant, EsadeGeo

Dario Arjomandi
Research Assistant, EsadeGeo

June 2026

Transparency and Disclosure Statement

This project received the support from Apple. In accordance with Esade's principles of academic independence and research transparency, all analysis, findings, interpretations, and recommendations were developed independently by the authors. The views expressed in this report are solely those of the authors and do not necessarily reflect the views of Esade, any sponsors, or any other institution with which they are affiliated. Sponsors bear no responsibility for the content of this publication or for any conclusions and recommendations contained herein.

Parts of this document were edited with the assistance of AI tools (ChatGPT and 365 Copilot) for language editing and stylistic refinement. All content has been critically reviewed and the authors take full responsibility for the final text.

Introduction

The **Digital Markets Act (DMA)** represents one of the most ambitious regulatory efforts undertaken by the European Union to reshape digital competition. Adopted in 2022 and fully applicable since May 2023, **the DMA introduces a proactive, ex-ante framework designed to ensure fair and contestable digital markets**. By defining a set of obligations for large online platforms known as **"gatekeepers" offering core platform services**, the regulation seeks to restrain structural imbalances, foster innovation, and protect consumers in an increasingly data-driven economy.

As implementation progresses, the full implications of the DMA are proving both complex and contested. Policymakers, scholars, and industry actors have raised important questions about its effectiveness, proportionality, and long-term impact on innovation, competitiveness, and user trust. The success of the regulation depends not only on how its obligations are enforced but also on **whether they achieve their intended goals while minimizing unintended economic or technological consequences.**

This policy brief, comes at a decisive moment, as the European Commission concludes its first review cycle of the DMA and stakeholders across Europe take stock of its early outcomes. The objective of this work is to analyze the DMA's early effects while incorporating the perspectives of key actors, including regulators, scholars, startups, and industry representatives. This policy brief also draws on the conclusions of a roundtable hosted by EsadeGeo in April 2026 on the Digital Markets Act and the tensions between competition, innovation, security and trust. The discussion brought together stakeholders from public institutions, regulators, policymakers, digital platforms, startup and SME representatives, industry, academia and legal and competition experts, ensuring a broad range of perspectives on the DMA's implementation across Europe's digital ecosystem.

This brief focuses on three interrelated themes that cut across both the academic debate and policy practice:

1. **Competition:** assessing whether the DMA's ex-ante obligations effectively increase market contestability or instead risk regulatory overreach.
2. **Innovation:** examining the DMA's effects on the incentives to innovation, research, development and the scaling of European startups.
3. **Data Security, Privacy, and User Experience:** exploring how to open digital ecosystems responsibly while protecting cybersecurity, usability, and user trust.

By examining the positive and negative effects of the Digital Markets Act across these themes, **this brief highlights the structural tensions at the core of the regulation, including the balance between fairness and flexibility, openness and security, and competition and innovation**. It identifies areas where recalibration may be needed to maximize the DMA's positive impact on Europe's digital economy and offers recommendations to support the refinement and effective implementation of the legislation.

Theme 1 - Competition
Ensuring Contestability Without Overreach

The Digital Markets Act marks a paradigm shift in European competition policy. By introducing ex-ante obligations for large digital platforms designated as "gatekeepers", it seeks to complement reactive antitrust enforcement with proactive regulation intended to secure contestable and fair markets. **This shift responds to long-standing concerns that traditional ex-post tools are too slow and too limited** to address entrenched digital markets' imbalances and reduce barriers to entry.

However, the same pre-emptive design that makes the DMA ambitious also introduces risks of overreach and market asymmetries; especially in light of the fact that its two main objectives, contestability and fairness, have not been operationally defined.

At its core, **the DMA seeks to lower structural market entry barriers by prohibiting self-preferencing, mandating data portability, and requiring interoperability with third-party services** through an ex-ante approach. That is, before any specific anti-competitive behaviour has been identified or reported. These ex-ante measures aim to expand opportunities for smaller business players and consumers while constraining the dominance of the largest companies. Yet, as highlighted by the literature (Colangelo & Ribera Martínez, 2025a; Bauer et al., 2025), **these obligations can have uneven effects across markets and technologies:** when applied uniformly to very different ecosystems, from mobile operating systems to online advertising, they may distort competition rather than restore it, especially if enforcement does not adequately reflect sector - specific dynamics. By applying identical obligations to all designated gatekeepers regardless of their market composition, business model, or systemic role, the DMA risks creating significant asymmetries. **Such uniformity risks to unevenly penalize differentiation**, which is one of the mechanisms through which firms compete on privacy, quality, and user experience. If regulatory obligations erode these distinctive advantages, **consumers may paradoxically face less meaningful choices.**

Additionally, concerns have been raised regarding the alleged complementarity of the DMA and ex-post competition law (Colangelo & Ribera Martínez, 2025b), on the grounds that ex-ante rules are considered to be less flexible and less capable of accommodating interpretations in response to technological evolutions. Moreover, some participants taking part at EsadeGeo's roundtable drew attention to the distinct objectives of the DMA and competition law-contestability and competition, respectively. **While contestability refers to the ability of third parties to overcome barriers of entry and compete with gatekeepers (recital 32 of the DMA),** competition concerns the absence of anti-competitive conducts that result from the abuse of a dominant position. As a result, a digital market may be competitive without necessarily being contestable. Under this view, the DMA does not merely complement existing competition law but actually goes beyond it, risking regulatory overreach.

Such an approach may also suggest that the DMA is mainly focusing on compliance with, and enforcement of, obligations, rather than on a concrete analysis of whether digital market dynamics harm potential competitors and consumers. **Formal compliance, such as changes to app store terms or ranking algorithms, does not necessarily translate into greater market access or consumer switching**. While Waldfogel (2024) highlights that the "Brussels effect" of the DMA is already visible in shaping global corporate behavior, compliance must be matched by empirical evidence of increased competition and innovation. Without robust metrics and indicators, there is a dual risk: premature tightening of rules before market effects are observable, and regulatory complacency based on procedural progress alone.

Defining clear indicators for contestability and fairness has implications for the EU as well as for other jurisdictions. If obligations are disproportionally prescriptive relative to their demonstrable effectiveness, they could export unintended market distortions abroad, potentially discouraging investment or innovation in Europe (Bauer et al., 2025).

Another area of concern is enforcement of DMA provisions. Although the European Commission retains exclusive competence for DMA enforcement, National Competition Authorities (NCAs) play a role in adjacent enforcement, as they can, among others, assume inspection and monitoring tasks if required to, and sometimes retain the power to refer (or not) investigations to the Commission, based on whether they consider the practices to be lawful or unlawful. Additionally, national courts have direct jurisdiction over disputes concerning the DMA. Scholars such as Ribera Martínez (2024) warn that **inconsistent interpretation among and within the various Member States could produce regulatory divergence and legal uncertainty**, while Bassini et al. (2025) signal that enforcing the DMA without adapting overlapping existing national and EU legislation can also result in fragmentation and lack of legal clarity. Ensuring coherence through structured coordination mechanisms, shared guidance, and a unified reporting framework will be essential to preserve the credibility and predictability of the Act.

Moreover, enforcement could be supported through clearer interpretative guidance, which would allow for practical design adjustments before reaching sanctioning measures. In April 2025, for example, the non-compliance investigation on Apple's iOS browser default-choice was closed after "a constructive dialogue" between the gatekeeper and the European Commission whereby the former adapted its browser choice screen (European Commission, 2025). The example illustrates how **structured technical dialogue may facilitate faster implementation adjustments and reduce uncertainty during compliance processes**, without prejudging enforcement outcomes. Further guidance would also provide more legal certainty and, consequently, reduce litigation and its associated costs. At the time of writing, the European General Court and Court of Justice of the EU have yet to rule on cases challenging the Commission's decisions involving Apple, ByteDance and Meta.

The DMA's success; namely, demonstrable improvements in contestability and fairness for markets and business and end users, as well as the elimination of fragmentation across Member States (recital 7 DMA) **will depend on whether enforcement remains flexible and evidence-based, focusing on measurable outcomes rather than procedures**. It will also require an ongoing dialogue between the European Commission, national institutions, industry, and civil society to recalibrate obligations as technologies and market structures evolve. In this sense, the DMA's most important innovation may lie in its capacity for adaptive governance, which learns and improves through practice.

The Commission's public summary of the DMA first-review consultations reflect a broad support, albeit not unanimous, for the DMA's objectives. However, it recognises that the DMA's real impact depends on enforcement that is timely, transparent, and well-resourced. Respondents including business users, SMEs, civil society and academics repeatedly cite slow processes, limited transparency, delaying tactics and interface modifications that do not introduce meaningful choice. These respondents call for interoperability "by design" supported by clearer technical standards, especially for messaging, operating systems and emerging AI-powered features. They also request better access to information, structured complaint channels and, in some cases, binding timelines, interim measures, independent audits, and compliance testing. Gatekeepers and gatekeeper-affiliated respondents, by contrast, emphasise the need for proportionality, legal predictability, and privacy concerns, preferring more enforcement and warning against inflexible obligations and high compliance costs (European Commission, 2026b).

Ultimately, the competition trade-off reflects a broader institutional dilemma: **how to discipline concentrated market power without stifling market dynamism**. An example of this tension is the evidence showing that EU users' searches on Google Maps increased by 21% after DMA modifications - removing clickable maps and direct links to Google Maps for EU queries (Pape & Rossi, 2026). The increase in searches mostly redirected users back to Google Maps rather than to alternative services. Other rivals saw no comparable increase in traffic, indicating weak competitive effects and continued user choice dominance. A contrasting illustration of this tension can be observed in the reported growth of alternative web browsers such as Aloha Browser, Opera and Vivaldi following the implementation of the DMA's browser choice obligations in March 2024. Aloha, a privacy-focused browser launched in 2016, reported a 250% increase in new EU users in the first month after the DMA became applicable (European Commission, 2026a). While causality cannot yet be conclusively established, these early developments suggest that **interoperability and user choice measures may contribute to greater visibility and adoption of alternative digital services.**

Policy Recommendations

Reinforce proportionality and consistency in enforcement through a coordination framework (e.g. enforcement board). Coordination between the European Commission and National Competition Authorities should be strengthened to ensure that oversight remains uniform across Member States. As highlighted by Ribera Martínez (2024) and Bauer et al. (2025), heterogeneous oversight risks eroding legal certainty and increasing compliance costs. A formal coordination framework or "DMA enforcement board" could promote consistent interpretations and avoid duplications with national rules. While coordination is currently channelled through the European Competition Network (ECN) - an institution originally established to enhance coordination in the field of competition law -, the creation of a formal framework specifically dedicated to the DMA, whether through a ECN Working Group or through an independent body, would contribute to a more consistent, unified and proportional enforcement.

Develop indicators of contestability and fairness. Current enforcement focuses on formal compliance rather than measurable market outcomes. Building on Waldfogel (2024) and Colangelo and Ribera Martínez (2025a), regular indicators (such as new entry rates, switching behavior, and access to APIs) could be published in an open portal to assess whether obligations genuinely foster contestability and fairness. To be effective, however, these concepts must be clearly defined in terms of their policy objectives. Particularly, an output- or results-oriented framing of contestability will directly shape how the concept is operationalised and measured. This would shift attention from procedural compliance to tangible results. Along these lines, in 2024, CERRE proposed the inclusion of output indicators in gatekeepers' reports to enable more robust future assessments. Implementing this approach requires acknowledging, by both the Commission and gatekeepers, that some results may challenge prevailing narratives (Feasey, Monti & de Streel, 2026), but would ultimately strengthen the DMA's effectiveness.

Shorten the DMA review cycle from three to two years. Given the rapid evolution of digital markets, formal reviews must be more frequent, without compromising legal certainty. A two-year review cycle, supported by continuous monitoring, would enable the European Commission to adjust obligations before structural damage to competitiveness or innovation occurs. This responds to Bassini et al. (2025)'s call for real-time evaluation and would allow for earlier identification and correction of unintended effects. The first review report under Article 53(1) of the Digital Markets Act was published on 28 April 2026, following a consultation process that included a targeted consultation launched in July 2025, as well as a call for evidence and a dedicated questionnaire on AI launched in August 2025. The review highlighted the speed at which digital markets are evolving, particularly in areas such as AI and cloud services, and emphasized the need for more agile and adaptive regulatory assessment cycles.

Formalize a channel for dialogue between regulators and gatekeepers. Regular communication channels between DG COMP, DG CONNECT and gatekeepers would enable early identification of implementation challenges, reducing litigation risks and fostering transparency. Structured dialogue would not compromise independence but would enhance regulatory agility. Including businesses and users in some of such formal dialogues could also contribute to more informed and effective enforcement.

Theme 2 – Innovation
Balancing Openness and Incentives

The Digital Markets Act aims to level the playing field by preventing dominant digital platforms, or gatekeepers, from unfairly favoring their own products or restricting access to key digital ecosystems. Yet this drive toward greater openness brings with it a complex trade-off for innovation incentives. **By requiring extensive interoperability, data sharing, and neutrality in self-preferencing, the DMA reshapes how companies decide where and how to invest in innovation**. The new rules affect their costs, risk profiles, and potential returns, pressing companies to rethink their long-term strategies for platform development.

The regulation's ex-ante nature means that interoperability obligations apply before any specific harm has been demonstrated. From an economic perspective, this proactive approach can prevent exclusionary behavior but may also constrain companies' ability to experiment with new business models. Several studies warn that openness by design, if applied uniformly across very different markets and services, **could weaken incentives for proprietary innovation, particularly in sectors that rely on high upfront R&D investment such as operating systems, mobile devices, and digital payments** (Cabral et al., 2021; Pettersson, 2022). In practice, companies might redirect innovation budgets away from experimental or high-risk projects toward compliance engineering and incremental adjustments, slowing the overall pace of technological differentiation.

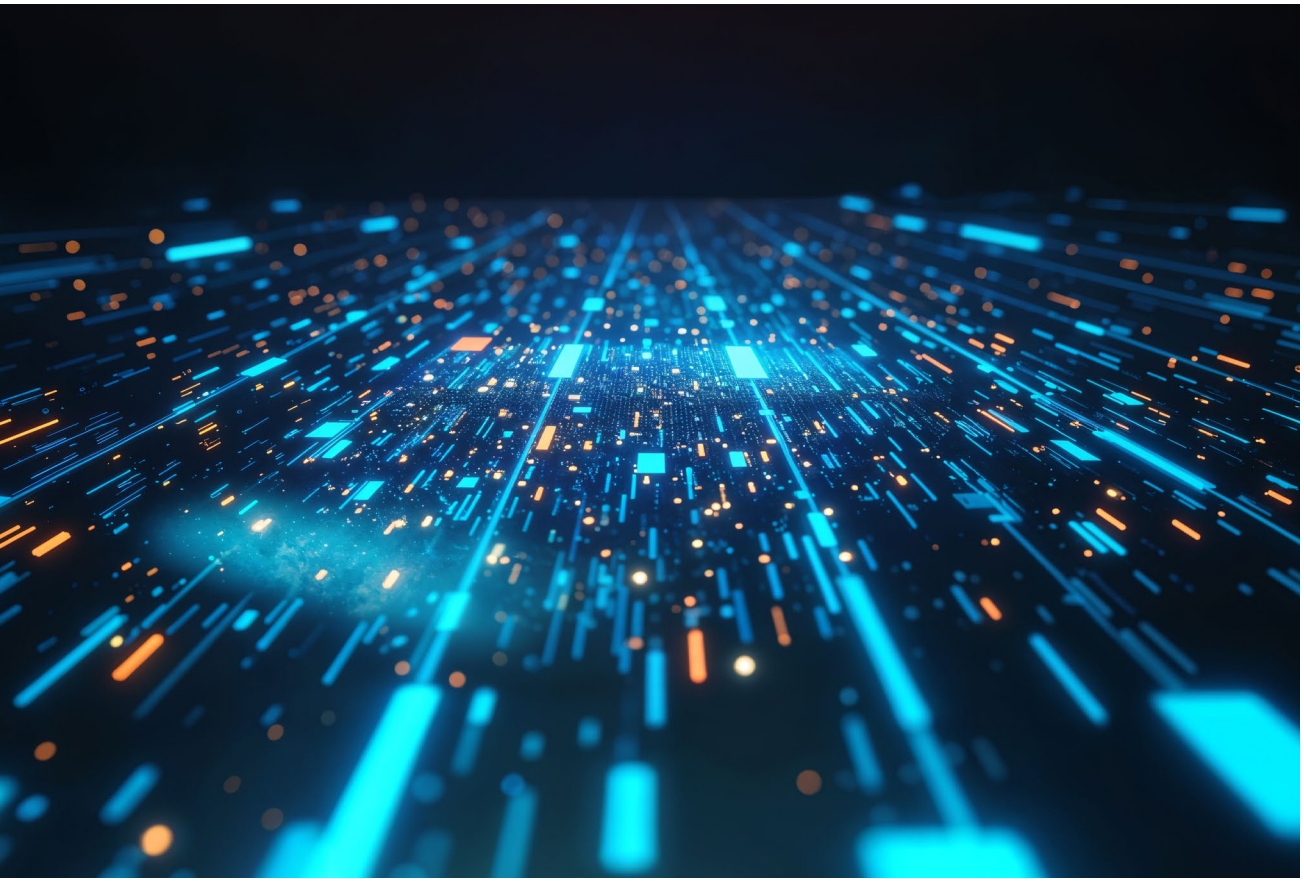
Interoperability obligations, outlined in articles 6 and 7 of the regulation, intend to create an incentive for new developers to innovate in features and functions that can be interoperable across core platform services. However, when indistinctively applied, these obligations can reduce the incentives of gatekeepers to produce or introduce innovation in core platform services, which are the basic digital infrastructure in many instances. In turn, SMEs and startups, which are the very actors the DMA intends to empower, face their own set of challenges. Interoperability and data-access rights create new openings for market entry, but **taking advantage of them often requires technical capacities that many SMEs cannot easily develop or sustain**. These challenges stem from the technical and legal complexity inherent in implementing interoperability obligations across heterogeneous digital ecosystems.

Article 6(7) of the DMA, on interoperability regarding hardware and software features accessed or controlled via the operating systems and virtual assistants is one of the most strategic provisions in this regard. Apple, Alphabet and Microsoft have provided processes for third parties to submit interoperability requests. **According to the European Commission's DMA Review, Apple has received more than 100 requests, and Alphabet has received more than 50**. The Commission argues that there is demand for interoperability solutions and forecasts that their gradual application will mobilize more demand in the future.

The Commission's review identifies that stakeholder views on interoperability remain divided. **Civil society organisations, SMEs and users support stronger interoperability by design, broader cross-platform mandates and open standards, including possible extensions** to communication services, AI-related technologies and cloud services.The Commission has clarified that such services may be designated as core platform services if they meet the relevant criteria, as they are considered to fall within the scope of the DMA.

At the same time, both gatekeepers and SMEs consider that interoperability obligations need to be proportional and distinctive, particularly in their implementation through specification procedures, guidelines and enforcement procedures. Even when obligations are ex-ante, **interoperability and openness might be proportionally calibrated and distinctly applied to different technology functions following, at least, two criteria: 1) demands for interoperability and 2) innovation risk or sectorial maturity**. Innovation risk can be measured taking into account elements such as the impact on cybersecurity integrity, on the incentives for capital intensive investments, on legal predictability and on the degree of exposure to overlapping regulations such as the Network and Information Security Directive (NIS2) and the Cyber Resilience Act (CRA).

As Simone and Laudando (2025) point out, the proportionality of DMA obligations is crucial, since excessive compliance complexity or insufficient implementation guidance could turn opportunities for new competitors into operational burdens for other smaller market players. Another dimension of these indirect effects on SMEs and startups is that their business development and competitive capacity is exposed to frequent changes of features in the core platform services on which they rely, especially in the case of OS and app stores. **In practice, frequent changes to APIs, interoperability conditions, access rules, or compliance-related functionalities can generate business uncertainty for smaller firms and app developers**. This uncertainty derives partly from the evolving enforcement environment and from the practical adaptation of compliance measures by gatekeepers, creating additional adjustment costs, and barriers to complementary innovation. Importantly, such risks are not uniform and they vary significantly across different core platform services and according to the specific functionalities involved.



The intellectual property (IP) dimension adds a layer of complexity. In an ex-ante regime, certain interoperability obligations can imply the disclosure of proprietary interfaces or functionalities, limiting a company's discretion to decide when and how to open its technologies. This raises potential tensions with the existing IP protection regime and may weaken the reward structures that sustain continuous innovation. If competitors can build upon a platform's core infrastructure without making equivalent investments or taking on similar risks, the incentive to pursue frontier innovation declines, a dynamic often described as the free-rider problem in innovation (Cennamo and Santaló, 2023; Lev-Aretz and Strandburg, 2020). Recent litigation before the EU General Court shows that the DMA's implementation also poses a legal question in its effects on proprietary technologies and fundamental property rights, and is relevant to establish the balance between contestability and the protection of property rights in digital markets.

With regards to the safety conditions for innovation, some SMEs and app developers rely on the safety and security standards provided by core platform services. Indistinctly applied interoperability could increase both compliance costs for gatekeepers (art. 6(4) DMA) and security oversight costs for SMEs in ensuring that open features continue to be secure. **Clearance costs would be further amplified with new platforms entering the market, which would also need to be evaluated**. This issue also raises the question of who bears the ultimate responsibility in case of any security breaches.

In terms of innovation, indistinctive interoperability applications can lead to compliance-driven design, where product decisions are shaped primarily by regulatory requirements rather than user needs or market differentiation. **In some cases, companies have delayed or limited feature releases in the European market because they cannot yet ensure DMA-compliant levels** of security or privacy across interoperable devices. Such delays create regional disparities in the availability of new features, ultimately resulting in a disadvantage to European consumers and developers.

Finally, the DMA's role as an instrument of economic policy may help create the market conditions necessary for innovative digital services to scale. However, an indirect competition approach alone is unlikely to be sufficient. **Open access conditions are more likely to translate into scalable innovation when combined with complementary industrial policy measures, including targeted financial instruments** –such as grants, investment instruments and public procurement– as well as broader structural reforms aimed at mobilizing capital and talent, including initiatives related to the Capital Markets Union and the ("28th regime") EU Inc.

At the same time, the relationship between openness and innovation is not one-dimensional. A growing body of research (Chesbrough, 2003; Gawer and Cusumano, 2014; Nambisan et al., 2017; Cennamo, 2021; European Commission, 2020) suggests that **well-governed open innovation ecosystems can stimulate complementary R&D and lower barriers to entry, accelerating innovation in emerging fields such as AI, quantum computing and digital health**. The DMA's long-term success may therefore depend not only on the degree of openness it creates, but on how interoperability obligations generate dynamic complementarities and proportionate incentives that continue to support investment in platform integrity, cybersecurity and proprietary R&D for all market actors.

In this context, the central policy challenge is one of calibration, sequencing and balance. The act's implementation ought to ensure that openness functions as a catalyst rather than a constraint by protecting intellectual property while enabling interoperability, supporting startups without imposing disproportionate compliance burdens, and providing the regulatory certainty necessary to sustain long-term investment and innovation.

Policy Recommendations

Calibrate the DMA's obligations based on innovation risk and sectoral maturity. Not all digital services and functionalities face the same risks of market dependency or competitive harm. DMA obligations should therefore reflect the principle of proportionality across two dimensions: the degree of interoperability required and the level of innovation risk or sectoral maturity involved. Obligations should be stricter where market dominance is entrenched and more flexible where technologies and business models remain emergent. Such a risk-based distinction would help ensure that the Digital Markets Act continues to promote innovation, investment and market contestability without inadvertently constraining the development of new digital services.

Protect IP rights within interoperability mandates. To prevent the erosion of proprietary innovation, guidance under Articles 6 and 7 could be provided to clarify how interoperability can be achieved without compromising core IP. Pettersson (2022) warns that overly broad interoperability obligations may unintentionally weaken IP protection and reduce incentives to innovate. A balanced framework that differentiates between functional layers and proprietary layers would help safeguard creativity while maintaining fair and equitable access. This approach would allow for equally effective but less restrictive measures to be implemented in order to protect IP in proprietary (essential) functions.

Introduce innovation sandboxes for DMA compliance experimentation. Given the technical and legal uncertainty surrounding interoperability obligations, the European Commission could explore the creation of voluntary and scoped experimental frameworks under the DMA. Controlled environments where startups and established firms test solutions compliant with the regulation, such as interoperability features, data-sharing mechanisms, or alternative app distribution models under supervision. This approach would provide legal certainty, reduce compliance risks, and generate evidence to inform enforcement and specification procedures, aligning with calls for more adaptive regulatory instruments (Simone and Laudando, 2025).

Align the DMA with EU economic policy and financing instruments. Aligning the DMA's market effects with the EU's economic policy and digital sovereignty objectives through policy reforms (Capital Markets Union, EU Inc) and financial instruments (grants, innovation funding programs, public procurement) that directly support the scaling of eligible digital projects and innovation. Specifically, the Commission could channel Horizon Europe or Digital Europe funds towards scaling up projects that develop secure interoperability, safe data-sharing, and fair platform models, in line with the Digital Decade target of doubling the number of high-value startups.

Theme 3 – Data Security, Privacy & User Experience

Balancing Openness with Integrity

The Digital Markets Act seeks to restore contestability and fairness in digital markets by curbing the structural advantages of dominant platforms. To that end, it mandates a series of openness obligations; **including third-party access to core services, the installation of alternative app stores, and data portability that are designed to reduce gatekeeper power and lower barriers** to entry for rivals. However, this shift introduces a fundamental and under-specified trade-off between expanding user choice and safeguarding the privacy, cybersecurity, and usability standards that underpin trust in digital systems. The central challenge is no longer whether to open ecosystems, but **how to ensure that openness is operationalized with integrity.**

A key insight emerging from both academic research and industry analysis is that **openness and security are not naturally aligned objectives. Obligations such as side-loading and mandatory interoperability can increase contestability, but they also expand the attack surface of devices and services, introducing new vectors for malware, fraud, and data leakage**. Interoperability mandated "free of charge" may unintentionally weaken incentives for upstream investment in secure infrastructure, while simultaneously increasing downstream risks for developers and users. As Bauer and Pandya (2025) argue, opening interfaces without clearly defined technical safeguards can generate unpredictable interactions across hardware and software environments, particularly in mobile ecosystems handling sensitive data such as biometric identifiers, geolocation, and financial information.

Importantly, interoperability is not a binary condition, but a spectrum. A critical distinction exists between technical interoperability (the formal ability to connect or switch) and real interoperability, which entails a seamless, secure, and user-friendly experience. **Systems may comply formally with interoperability obligations while, in practice, offering degraded functionality, limited compatibility** with the latest features, or complex switching processes. In such cases, openness exists in theory but fails to translate into meaningful user empowerment or competitive pressure. This raises a core enforcement challenge: how to move from formal compliance to effective, user-centric interoperability; a distinction that Feasey, Monti and de Streel (2026) identify as central to any credible assessment of the DMA's impact.

From a security perspective, extending interoperability obligations risks opening systems to cyberattacks and malware, particularly in contexts where responsibility for system integrity becomes diffused. Opening systems increases not only technical complexity; such as versioning and compatibility issues, but also uncertainty regarding liability when breaches occur. Developers, especially smaller ones, may face rising costs to monitor vulnerabilities, detect copycat applications, and ensure compliance across multiple distribution channels. In parallel, gatekeepers remain accountable under cybersecurity frameworks such as the CRA and NIS2, even as they are required under the DMA to open their systems to third parties. This creates a structural tension: **firms may be required to open their systems while retaining responsibility for risks they no longer fully control.**

These concerns are particularly acute for gatekeepers **whose product architectures rely on hardware-based encryption and tightly controlled software environments to ensure end-to-end security**. From this standpoint, side-loading and mandatory interoperability may introduce components that cannot be fully audited, thereby weakening system integrity. The delayed or restricted rollout of certain features in the EU market has been cited in some cases as a direct consequence of this regulatory uncertainty (for instance, Apple delayed the launch of its AI-powered Live Translation feature for AirPods in the EU due to the additional engineering work required to comply with interoperability obligations under the DMA, while Meta postponed the launch of Threads in the EU amid uncertainty around data-sharing and compliance with EU digital regulations, including the DMA (Apple, 2026; Milmo, 2023). Not all delays can be attributed solely to regulation, but evidence suggests that **compliance requirements are increasingly a contributing factor in later product rollouts in Europe** (Markeviciute, 2025). While such claims require empirical scrutiny, they highlight the broader issue that regulatory design can shape not only market structure, but also product development and feature availability in specific jurisdictions.

The interaction between the DMA and the General Data Protection Regulation (GDPR) introduces an additional layer of complexity, particularly in relation to data sharing and user consent. Interoperability often requires data flows across services, triggering consent requirements that may be repetitive, fragmented, or difficult for users to understand. There is a **growing risk of "consent fatigue",** whereby users are repeatedly prompted to authorize data processing without meaningful comprehension, ultimately defaulting to pre-selected options. This dynamic undermines the very objective of user empowerment. Moreover, as de Streel and Monti (2026) demonstrate, **the concept of "consent" is not uniformly defined across** the DMA, GDPR, and Digital Services Act (DSA), creating legal ambiguity and increasing the risk of divergent interpretations across Member States. In practice, formal compliance with consent requirements may coexist with poor user understanding and limited real agency.

Beyond consent, the user experience dimension represents a critical and often underestimated factor. Trust is best understood as a function of both perceived security and usability. If interoperability leads to confusing interfaces, degraded performance, or increased exposure to fraud, **users may rationally choose to remain within familiar, closed ecosystems**. In this sense, usability, privacy, and security are not competing goals but interdependent conditions for effective contestability. Poorly designed user journeys, whether in switching mechanisms, consent flows, or app installation processes **can neutralize the competitive benefits that the DMA seeks to unlock.**

There is also a broader need to reconsider how consent and data governance are operationalized. One promising avenue is the development of persistent or system-level consent architectures, such as browser- or operating system-based privacy profiles that allow users to set preferences once, rather than repeatedly across services. While such approaches may improve usability and reduce consent fatigue, they also raise new concerns about the concentration of control at the infrastructure level, potentially reinforcing the power of operating system providers. This illustrates a broader point: **solutions to fragmentation risks may themselves create new forms of centralization, requiring careful regulatory calibration**. Any such architecture would also require careful governance design regarding liability allocation, user autonomy, interoperability standards, and consistency with GDPR principles.

Finally, the question arises whether interoperability should be imposed uniformly across all services and functionalities. The current DMA framework largely assumes openness by default, yet a more demand-driven and proportional approach may be warranted; one where interoperability obligations are calibrated based on actual demand, security risks, and the sensitivity of the data or functionality involved (Euroconsumers Group, 2025). **Not all features may require immediate or full interoperability, particularly where this could compromise privacy, security, or innovation incentives**. This suggests that flexibility and contextualization should play a greater role in future implementation and review cycles.

Policy Recommendations

The analysis above points to five concrete areas where policy action is needed to ensure that the DMA's openness obligations deliver meaningful, trustworthy, and durable outcomes.

Establish minimum security standards as a precondition for interoperability compliance. Interoperability obligations should not be treated as unconditional and should instead be calibrated depending on multiple factors, notably security standards. Developing a baseline framework of technical security requirements - including vetting procedures, vulnerability disclosure standards, and audit rights that third parties must meet before gaining access to gatekeeper systems - could help to address these concerns. The Commission, in coordination with the European Union Agency for Cybersecurity (ENISA) and national cybersecurity authorities, could support or facilitate the development of this framework. This would address the structural tension between DMA openness obligations and the accountability requirements under the CRA and NIS2, and provide clearer liability allocation in the event of breaches.

Define and enforce effective interoperability, not merely formal compliance. Enforcement practice should move beyond verifying whether gatekeepers have technically opened their systems, and towards assessing whether the resulting interoperability is genuinely seamless, secure, and user-friendly. By developing measurable, user-centric indicators of effective interoperability covering switching ease, feature parity, and interface quality and integrating these into compliance assessments and specification proceedings, the Commission could contribute to more effective and user-friendly interoperability. As Feasey, Monti and de Streel (2026) argue, compliance and impact are distinct, and enforcement frameworks must reflect that distinction.

Resolve cross-regulatory incoherence on consent and data governance. The divergent treatment of "consent" across the DMA, GDPR, and DSA is a source of legal uncertainty that undermines both regulatory effectiveness and user trust. Establishing clear priority rules for cases of overlap and conflict, and coordinating more closely across the enforcement bodies responsible for each regime through the publishing of structured coherence strategies, would facilitate a consistent treatment of consent obligations across EU legislation (Streel and Monti, 2026).

Embed user experience as a first-order metric of DMA success. Trust is a precondition for competitive switching, and poor user experience can neutralize the contestability benefits the DMA seeks to generate. Policymakers should treat usability, alongside security and privacy, as a substantive regulatory objective, not an afterthought. Policymakers should explore the viability of persistent or system-level consent architectures that reduce fragmentation and consent fatigue without concentrating excessive control at the infrastructure level. This means incorporating user experience assessments into DMA review cycles, ensuring that switching mechanisms, consent flows, and alternative distribution channels are designed to genuinely serve users rather than merely satisfy formal obligations. Such assessments could rely on independent consumer research bodies, standard-setting organisations, academic institutions, or multi-stakeholder expert panels to complement policymakers' direct regulatory evaluation.

Taken together, these recommendations point to the need for a governing policy concept of *secure interoperability*; a framework that enables openness and user choice while embedding robust safeguards for privacy, cybersecurity, and user experience. Secure interoperability is not merely a technical challenge, but a governance imperative that must address liability allocation, certification standards, user interface design, and cross-regulatory coherence. Without such an approach, there is a risk that the DMA will either overcorrect (undermining trust and security) or underdeliver (failing to generate meaningful competition). Whether the DMA achieves its objectives will depend in large part on how these trade-offs are managed in practice. Openness that erodes trust or degrades user experience risks undermining the very contestability the regulation is designed to foster. A governance framework that treats security, usability, and privacy as integral to (rather than in tension with) the DMA's competition objectives is therefore necessary for effective implementation.

Cross-Cutting Recommendation

Institutionalize continuous monitoring and transparency. Establish transparent metrics on DMA implementation outcomes, providing systematic and comparable information on indicators such as market entry, user traffic metrics, innovation output and enforcement actions. Making this data publicly available would increase transparency and accountability, allowing policymakers, researchers, and industry actors to monitor how the regulation is shaping digital markets in real time. This would also create a shared empirical evidence base to inform future review cycles, helping the Commission refine obligations, assess proportionality, and identify unintended effects at an early stage.

Conclusion

Looking ahead, further **improvements and refinements to the Digital Markets Act may not require major amendments to the regulation as a whole**. The regulation's core objectives of fairness and contestability, together with its gatekeeper designation framework, remain well-founded. **Its ex-ante obligations have already produced early results**: platforms are opening up, user choice is broadening, app distribution is becoming less constrained, and self-preferencing practices are being corrected. Yet without structured measurement indicators, the broader impact on market dynamics and on the wider digital ecosystem remains difficult to assess beyond individual cases.

At the same time, the implementation of these obligations carries risks of unintended or counterproductive effects in the medium term. Tensions have emerged between the DMA's ex-ante framework and existing competition, intellectual property, and data protection law. **There are also risks of weakened innovation incentives for both gatekeepers and SMEs, alongside emerging challenges related to cybersecurity, user experience, and developers' operational conditions.**

Addressing these risks does not require waiting for major legislative revision. **Drawing on the experience accumulated through specification procedures, enforcement actions, litigation, and the recent Commission review**, targeted adjustments are possible within the existing framework. Two priorities stand out. First, strengthening institutional coordination and fostering structured dialogue among national and European authorities, gatekeepers, and SMEs, and across legal regimes, is essential to reduce the risk of unintended effects and improve coherence. Second, **establishing an impact assessment framework would generate the empirical evidence needed to evaluate outcomes** and inform proportionate policy responses over time.

More specifically, **introducing greater differentiation and proportionality in the definition and enforcement of interoperability** obligations would help balance open access, competitive capacity, legal certainty, and user experience; and thus mitigating risks to innovation without compromising the DMA's core objectives. These adjustments could be gradually **reinforced through complementary economic policy instruments designed to align market actors' strategies** with both the evolving outcomes of the DMA and the European Union's broader digital sovereignty ambitions.

Bibliography

Apple. (2025, November 4). Live Translation on AirPods expands to the EU [Press Release]. Apple Newsroom. Retrieved May 18, 2026 from https://www.apple.com/ie/newsroom/2025/11/live-translation-on-airpods-expands-to-the-eu

Bassini, M., Maggiolino, M., & de Streel, A. (2025). *Better law-making and evaluation for the EU digital rulebook*. CERRE. https://cerre.eu/publications/better-law-making-and-evaluation-for-the-eu-digital-rulebook

Bauer, M., & Pandya, D. (2025). *Cybersecurity at risk: How the EU's Digital Markets Act could undermine security across mobile operating systems*. ECIPE. https://ecipe.org/blog/dma-gift-to-hackers-threat-to-competition/

Bauer, M., Pandya, D., & Sharma, V. (2025). *EU export of regulatory overreach: The case of the Digital Markets Act (DMA)*. ECIPE. https://ecipe.org/publications/eu-export-of-regulatory-overreach-dma/

Cabral, L., Haucap, J., Parker, G., Petropoulos, G., Valletti, T., & Van Alstyne, M. (2021). *The EU Digital Markets Act: A report from a panel of economic experts*. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122910/jrc122910_external_study_report_-_the_eu_digital_markets_acts.pdf

Chesbrough, H. W. (2003). Open innovation: *The new imperative for creating and profiting from technology*. Harvard Business School Press.

Cennamo, C. (2021b). Digital Markets Act's objectives: Efficiency vs. innovation logics. In L. Wiewiorra & I. Godlovitch (Eds.), *The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/662930/IPOL_IDA(2021)662930_EN.pdf

Cennamo, C. (2021a). Competing in digital markets: A platform-based perspective. *Academy of Management Perspectives*, 35(2), 265–291. https://doi.org/10.5465/amp.2016.0048

Cennamo, C., Kretschmer, T., Constantinou, I., & Garcés, E. (2025). *Economic impact of the Digital Markets Act on European businesses and the European economy*.

Cennamo, C., & Santaló, J. (2023). Potential risks and unintended effects of the new EU Digital Markets Act. EsadeEcPol. https://www.Esade.edu/ecpol/wp-content/uploads/2023/02/AAFF_EcPol-OIGI_PaperSeries_04_Potentialrisks_ENG_v5.pdf

Cisnal de Ugarte, S., Fleischer, R., & Hickey, E. (2025). *The Digital Markets Act: A procedural journey towards effective compliance*. K&S / CCIA Europe. https://www.kslaw.com/attachments/000/013/012/original/A_Procedural_Journey_Towards_Effective_Compliance.pdf

Colangelo, G., & Ribera Martínez, A. (2025a). The metrics of the DMA's success. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.4

Colangelo, G. & Ribera Martínez, A. (2025b).Vertical interoperability in mobile ecosystems: Will the DMA deliver (what competition law could not)? *International Review of Law & Economics*, 83. https://doi.org/10.1016/j.irle.2025.106267

Cseres, K. J., & de Korte, L. C. (2025). Participation of third parties in the public enforcement of the Digital Markets Act: Between democracy and technocracy. *Journal of Antitrust Enforcement*. https://doi.org/10.1093/jaenfo/jnae051

de Streel, A., & Monti, G. (2026). *DMA regulatory interplays*. CERRE. https://cerre.eu/publications/dma-regulatory-interplays/

Euroconsumers Group. (2025). *Reimagining interoperability*: A proposal for horizontal obligations under the Digital Markets Act. https://www.euroconsumers.org/wp-content/uploads/2025/09/Reimagining-interoperability-a-proposal-for-horizontal-obligations-under-the-Digital-Markets-Act.pdf

European Commission. (2020). Commission Staff Working Document: Impact Assessment Report accompanying the document Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0363

European Commission. (2025, April 23). *Commission closes investigation into Apple's user choice obligations and issues preliminary findings* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1086

European Commission. (2026a). *Commission staff working document accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the review of Regulation (EU) 2022/1925 … Digital Markets Act, in accordance with Article 53 thereof* (SWD(2026) 123 final). https://digital-markets-act.ec.europa.eu/document/download/788ff6d9-f0bf-47d2-80a8-611d5ee5bc51_en?filename=DMA%20Review_Commission%20Staff%20Working%20Document_SWD_2026_123_1_EN.pdf

European Commission. (2026b). *DMA review: Summary of consultation contributions*. https://digital-markets-act.ec.europa.eu/document/download/244d8f93-e969-41af-bdcc-23e791863449_en?filename=Public%20summary%20of%20DMA%20Review%20consultation_0.pdf

Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. *Journal of Product Innovation Management*, 31(3), 417–433. https://doi.org/10.1111/jpim.12105

Feasey, R., Monti, G., & de Streel, A. (2026). *Assessing and improving the DMA's impact*. CERRE. https://cerre.eu/publications/assessing-and-improving-the-dmas-impact/

Lev-Aretz, Y., & Strandburg, K. J. (2020). Regulation and innovation: Approaching market failure from both sides. *Yale Journal on Regulation Bulletin*. https://www.yalejreg.com/bulletin/regulation-and-innovation-approaching-market-failure-from-both-sides/

Markeviciute, E. (2025, September 26). Consumer waiting game: Why do tech products launch later in Europe? *Euronews*. https://www.euronews.com/next/2025/09/26/consumer-waiting-game-why-do-tech-products-launch-later-in-europe

Milmo, D. (2023, July 5). Meta delays EU launch of Twitter rival Threads amid uncertainty over personal data use. *The Guardian*. https://www.theguardian.com/media/2023/jul/05/meta-delays-eu-launch-of-twitter-rival-threads-amid-uncertainty-over-personal-data-use

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. *MIS Quarterly*, 41(1), 223–238. https://doi.org/10.25300/MISQ/2017/41:1.03

Pape, L.-D., & Rossi, M. (2026). Is competition only one click away? The Digital Markets Act's impact on Google Maps. *Marketing Science*. https://pubsonline.informs.org/doi/10.1287/mksc.2025.0159

Pettersson, D. (2022). *Sector-specific ex ante regulation in digital markets: A complement or substitute to antitrust enforcement?* SSRN. https://ssrn.com/abstract=4222013

Ribera Martínez, A. (2024). The decentralisation of the DMA's enforcement system. *GRUR International*. https://doi.org/10.1093/grurint/ikae139

Simone, C., & Laudando, A. (2025). Principles and obligations of the Digital Markets Act in regulating the economic power of gatekeepers: Positive, negative or trade-off effects? *Electronic Markets*. https://doi.org/10.1007/s12525-025-00788-6

Vezzoso, S. (2024). *"Super-apps" and the Digital Markets Act*. arXiv. https://doi.org/10.48550/arXiv.2404.04506

Waldfogel, J. (2024). *Amazon self-preferencing in the shadow of the Digital Markets Act.* National Bureau of Economic Research. https://www.nber.org/papers/w32299