cerre

DMA@2: TOWARDS STRONGER GOVERNANCE AND EVALUATION?

BOOK

April 2026

Alexandre de Streel
Marc Bourreau
Richard Feasey
Jan Krämer
Zach Meyers
Giorgio Monti

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this book has been prepared, received the support and/or input of the following CERRE member organisations: ACM, Amazon, Apple, Arcep, DuckDuckGo, EETT, Google, Mozilla, Qualcomm. However, they bear no responsibility for the contents of this book. The views expressed in this CERRE book are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

Executive Summary

This book presents the outcomes and findings of the CERRE Digital Markets Act Implementation Forum 2025. The Forum serves as a neutral and trusted platform for dialogue among stakeholders affected by the DMA, including gatekeepers, business users, and end users, as well as representatives of the regulatory authorities.

The 2025 edition of the Forum aims to inform the European Commission's ongoing review of the DMA. It is structured around four issue papers, which are briefly summarised in this executive summary. These papers address: (i) the need to develop a robust evaluation framework for the DMA; (ii) the potential extension of horizontal interoperability obligations to social networks; (iii) the development of governance mechanisms to ensure the effective opening of digital platforms; and (iv) the need to better address the interplay between the various instruments of the EU digital regulatory framework.

1. Developing a robust framework to evaluate the DMA

The first issue paper discusses how the European Commission should approach the assessment of the impact of the Digital Markets Act (DMA) on digital markets and considers how the results should inform its enforcement practices.

The gatekeeper compliance reports, European Commission annual reports, and other ad hoc studies produced to date do not provide a good basis for understanding the impact of the DMA. This reflects an **early focus on obtaining compliance rather than assessing impact**. It suggests that those affected by the DMA have limited incentives to collect or voluntarily share the sort of data required to undertake an evaluation. The paper recommends that this is addressed by the **European Commission obliging the gatekeepers to collect and report data**, and it suggests that 'output indicators' provide an initial list of the data that should be provided, although this might be supplemented with other data from other sources. Although compliance will also remain ongoing, the paper argues that the **assessment of impact should not wait until full compliance is achieved, since the processes are interdependent**.

The European Commission has yet to **develop or define a robust evaluation framework which it would use to assess the impact of the DMA and which the data it is recommended to collect** would populate. The approach taken in the Impact Assessment undertaken for the DMA proposals in 2020 is not fit for this purpose, and assessments of other legislation, such as the General Data Protection Regulation (GDPR), have not met the requirements of the Better Regulation Guidelines. It is unrealistic to expect a proper framework to be in place for the first assessment, which is to be completed by May 2026; however, work should start now with a view to having a framework by the next review in 2029.

This timing is appropriate because the impact of the **DMA will take some years to become fully apparent**. This is partly because compliance remains an ongoing process, but also because it will involve significant changes in the way in which gatekeepers behave, which will take end users and business users time to fully understand and respond to.

The paper outlines the **benefits and costs which a robust evaluation framework would need to take proper account of**. These include:

- Benefits that might arise from greater competition in the provision of services which rely upon access to core platform services enabled by the DMA, or from greater competition or the threat of competition to the core platform service itself. This would include not only the choice of new services but also improvements which the gatekeepers make to their services in response to competition, or positive changes to new services that must now comply with the DMA.
- Benefits when end users are better able to access the services they prefer, whether as a result of lower switching costs or by exercising rights to withhold data and protect their privacy.
- Benefits when business users are able to use better advertising or transaction services in conjunction with the core platform service as a result of the DMA, to obtain better terms of trade from the gatekeepers themselves, or to more readily multi-home or switch between platforms.
- Ongoing costs incurred by the gatekeeper to comply with the DMA.
- Costs that might arise if the DMA forces a gatekeeper to delay a new service, not develop it, or adapt it in ways that are harmful for some end users (notwithstanding competitive pressures to the contrary).
- Costs to end users if the DMA reduces differentiation in services in ways that mean some end user preferences are no longer met, or are met less well.

The purpose of evaluating the impact of the DMA in the way proposed is to **allow a consensus to develop about the impact of different combinations of core platform services and DMA obligations**. This should then allow the European Commission to focus its compliance and enforcement efforts on those which are most beneficial, and to reconsider those which impose costs overall. It will take time for any consensus to develop and for the framework to mature. The paper recommends the steps that need to be taken to start this process.

The paper also recommends **steps the European Commission could take to improve the impact of the DMA over time**. One is that the European Commission should begin to provide **greater clarity** about when compliance is achieved and what is required from the gatekeeper to achieve it. This might be difficult at the initial stages of implementation, but ought to improve over time. Another is that the European Commission should seek to **improve the coherence between different obligations** as they apply to the same core platform service. The paper highlights examples where different obligations pull in different directions – for example, by aiming to promote competition within a platform (and so making it more attractive to users), whilst at the same time seeking to encourage entry by rival platform providers (who might be deterred from entering if the incumbent platform becomes more attractive or prices fall), or when the same obligation benefits some business users but harms others. Finally, **other jurisdictions** such as the US are beginning to implement measures which have similar aims to those pursued by the European Commission through the DMA. The European Commission might have something to learn from their experiences as to the impact of different measures and different approaches.

2. No need to extend horizontal interoperability obligations to social network services

In its upcoming DMA review, the European Commission should also consider whether to extend the horizontal interoperability obligations to Social Networking Services. Social networks are inherently

more complex and differentiated than interpersonal communications services, to which such obligations already apply and whose implementation has proven challenging in practice.

The expected impact of horizontal interoperability on competition and contestability in social network markets appears limited. For social networks, interoperability can realistically only encompass a subset of standardised functionalities. As a result, key sources of market power, such as network effects and installed-base advantages, are likely to remain largely unaffected. Importantly, multihoming—whereby users engage with multiple social networks in parallel—already constitutes a viable competitive dynamic and provides an alternative pathway for new entrants to build a user base. Mandated interoperability may inadvertently reduce users' incentives to multi-home by reinforcing the role of dominant platforms as central access points, thereby potentially weakening, rather than strengthening, market contestability.

In addition, extending horizontal interoperability would **entail significant implementation costs** and require continuous regulatory oversight, while **raising complex security and integrity concerns**. These burdens should be carefully weighed against the likely benefits. Finally, there is a risk that interoperability could amplify existing societal harms associated with social networks, including the spread of disinformation, hate speech, privacy risks, and addictive usage patterns, by facilitating the cross-platform dissemination of harmful content.

Overall, extending horizontal interoperability obligations to social networking services is unlikely to generate substantial competitive benefits and may introduce disproportionate technical, security, and societal risks.

3. Developing technology and governance mechanisms for opening the tech platforms

While the DMA sets out high-level platforms and data access obligations, it is largely silent on the technical, commercial, and governance mechanisms required to make portability and interoperability work in practice. Each of these obligations raises complex implementation questions. Decisions must be taken about which data and functionalities fall within scope; how data should be formatted and transmitted; how interfaces, APIs and user-facing tools should be designed; how security and privacy can be maintained; and how quality, reliability and continuity of access should be ensured. These technical choices have a range of implications for gatekeepers' and third parties' investment incentives, for competition, and for users' willingness and ability to take advantage of portability and interoperability in practice.

Security deserves particular note. The draft joint guidelines of the European Commission and the European Data Protection Board illustrate the tension between security and contestability, particularly in relation to the extent to which gatekeepers may assess or rely on the trustworthiness of third-party data recipients. This third issue paper argues that a proportionate approach is essential, recognising that **security screening may have some role, while preventing security justifications from being used to frustrate contestability**.

Without clearer expectations around service levels, documentation, notice periods for changes, and interface stability, business users may lack the confidence to invest in building interoperable services. Experience from other regulated sectors suggests that **quality standards and key performance indicators are often as important as access rights themselves**.

Given the volume of discretionary decisions involved, governance mechanisms – that is, the processes by which decisions about implementing openness are made – play a critical role. To date, DMA implementation has largely followed a gatekeeper-led model, with platforms proposing bespoke solutions subject to Commission oversight. In a few cases, the Commission has adopted a more proactive approach of specifying how gatekeepers must comply. While these approaches have been understandable in the early days of DMA implementation, they may not be the optimal approach in the long run. The paper therefore explores the **potential for more collective and inclusive governance mechanisms, involving structured dialogue between gatekeepers, business users, regulators and relevant public authorities**. Such mechanisms could improve transparency, promote balanced decision-making, and gradually encourage greater consistency across platforms, without resorting prematurely to standardisation. However, inclusive governance also raises challenges around participation, speed of decision-making, and the risk of constraining innovation if consensus requirements are poorly designed.

The paper concludes that no single governance model is appropriate for all DMA obligations or all types of platform services. Instead, the **Commission should encourage a graduated shift towards more transparent, inclusive and institutionalised governance, tailored to the maturity and risk profile of different services**. This includes clearer documentation of available functionalities and data, standing forums for dialogue, predictable change management processes, objective access criteria, and greater use of trusted third-party intermediaries such as data transfer initiatives and trust registries. Over time, these mechanisms can help ensure that openness under the DMA becomes not only legally enforceable, but practically usable, economically viable, and a credible basis for third parties to invest and innovate.

4. Maximising the regulatory synergies within the EU digital rulebook

The last issue paper calls for a structured strategy to ensure coherence across the EU digital rulebook, with particular attention to the implementation of the Digital Markets Act (DMA). **As overlaps between the DMA and instruments such as the Digital Services Act (DSA), IP laws or the General Data Protection Regulation (GDPR) become more operationally significant, policymakers should adopt clear interpretative guidance that identifies synergies, mitigates tensions, and transparently manages unavoidable trade-offs**. Joint guidelines—developed through open and participatory processes—should go beyond aggregating institutional positions and instead provide practical compliance pathways, clarify proportionality standards, and specify where safe harbours may apply. In particular, structured frameworks are needed to reconcile DMA interoperability and data-access obligations with intellectual property rights and data protection requirements, ensuring that enforcement remains both effective and innovation-friendly.

To reduce regulatory fragmentation, this issue paper recommends **strengthening institutional coordination and rationalising overlapping obligations**. Legislative simplification through targeted omnibus reforms should eliminate redundant rules while preserving substantive protections, and future initiatives could consolidate enforcement cooperation across the more than 270 EU and national bodies involved in digital oversight. The Commission's planned "digital fitness check" should be grounded in rigorous, evidence-based evaluation of the DMA's impact, supported by systematic data collection and a dedicated assessment framework. In parallel, enforcement practices should

prioritise EU-level solutions where conduct is cross-border in nature, limiting the risk of divergent national remedies and gold-plating that increase compliance costs and weaken the internal market.

With respect to data protection, the issue paper recommends **operationalising coherent parallel application of the DMA and GDPR**. Clear workflows should be developed to guide cooperation between gatekeepers and business users, for instance in areas such as consent management and data portability. Regulators should promote tested, user-friendly choice architecture and require gatekeepers to substantiate how compliance designs achieve legal objectives. Where guidance suggests specific compliance measures, authorities should clarify whether these create presumptions of compliance and ensure that recommendations are proportionate and grounded in a clear legal basis.

Finally, the issue paper highlights the **need for more governance of enforcement**. Enhanced dialogue among regulators should aim to produce unified compliance solutions rather than duplicative or conflicting remedies. In the medium term, more structured and pragmatic regulatory cooperation with initiatives like the Digital Clearing House 2.0 should be encouraged. In the longer term, policymakers may consider the establishment of an independent EU digital enforcement agency to ensure consistency and effectiveness. In private enforcement, national courts should coordinate closely with the Commission and exercise caution when granting injunctive relief, preserving the DMA's principle that gatekeepers retain discretion in designing compliance unless specific remedies are strictly necessary.

Table of Contents

Assessing and Improving the DMA's Impact

Richard Feasey
Giorgio Monti
Alexandre de Streel

1. Introduction

This issue paper discusses how to assess the **impact of the DMA[1] and how the European Commission might approach its enforcement practices in light of that assessment.** The Commission is currently undertaking its first review of the implementation of the DMA, as required by Article 53, and this paper is intended to inform that review. The issues identified and findings made in this paper are based upon interviews that we have conducted with a number of gatekeepers and business users, together with our analysis of submissions made as part of the Commission's first DMA review,[2] compliance reports produced by gatekeepers (as required by Article 11 DMA),[3] the annual reports published by the Commission (as required by Article 35),[4] and other materials produced by the industry associations or civil society organisations. The views presented in this paper are entirely our own.

The positive and negative impact of a particular obligation as implemented by a particular gatekeeper for a particular core platform service will depend upon, amongst other things, whether, or to what extent, the measures taken by that gatekeeper amount to 'effective compliance'. In interviews, we received information on why some business users consider compliance remains incomplete for some obligations and suggestions that this explained the limited impact of the DMA. We have said previously that **we think the assessment of compliance and the assessment of impact, although they are linked, can be approached as discrete questions** as there is no particular or necessary set of service output or market outcomes that will tell the Commission that a gatekeeper has achieved effective compliance.[5] The DMA makes a similar distinction insofar as the requirement for the Commission to produce an annual report on implementation of the DMA and the progress made towards achieving its objectives (under Article 35) is separate from the requirement (under Article 53) to undertake a three-year review that evaluates the impact of the DMA. We emphasise that we do not take any position in this paper as to whether a particular gatekeeper has complied with a particular obligation or as to the overall level of compliance with the DMA**.** We also consider that an assessment of impact, which is the focus of this paper, need not await a finding that a gatekeeper is effectively complying with a particular obligation and that the two processes should be pursued in parallel.

The Commission's focus to date has been, understandably, on improving compliance whilst progress on assessing impact has been very limited. Thus, the Commission's second annual report makes only very limited reference to the impact of implementation to date and is mainly a description of the actions the Commission itself has taken. Similarly, the compliance reports published by the gatekeepers are largely descriptions of the actions they have taken to comply with the obligations in the DMA rather than any assessment of how business users or end users have responded. The outcome of the Commission's first review will, we assume, begin to fill the assessment gap but a lot more work remains to be done. Therefore, one of the main calls of this issue paper is for the Commission to begin to develop a solid and comprehensive evaluation framework using data and other evidence to be provided by the gatekeepers and other involved stakeholders. This framework will not be completed for the review which must be completed by May 2026, but work should start as

[1] Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1.
[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14831-Review-of-the-Digital-Markets-Act_en
[3] https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports
[4] https://digital-markets-act.ec.europa.eu/about-dma/dma-annual-reports_en
[5] https://cerre.eu/publications/dma-implementation-forum/

soon as possible if it is to inform the next Review which must be completed by 2029. This may allow the Commission to identify ways to make the DMA a more targeted, proportionate and effective regime.

Another important and more immediate theme of this paper is to make some recommendations to **facilitate compliance and increase the impact of the DMA.** This can be achieved by increasing legal predictability and compliance acceptability with the DMA obligations, by improving legal coherence among the DMA obligations and by maximising the synergies with regulatory practices in other jurisdictions.

2. Developing a robust evidence base

2.1. The publicly available data

2.1.1. DMA review consultation

The evidence currently in the public domain that would allow us to assess the impact of the DMA is very limited.[6] This means that the merits of the DMA continue to be debated in largely rhetorical terms, and claims are assertions rather than being based on real-world data. In this we broadly agree with another commentator's assessment of the submissions made by gatekeepers, business users and civil society groups in response to the Commission's consultation for the DMA review:

> *The Digital Markets Act pursues two objectives: ensuring digital markets are contestable and fair. Article 53 requires the Commission to assess whether these objectives are being achieved. Yet the consultation submissions reveal a fundamental problem: stakeholders are engaged in advocacy, not analysis. The evidence bases for assessing the DMA's impact are remarkably thin, and what evidence exists is contested, partial, and often impossible to verify.*
>
> *The submissions are characterized by assertion rather than substantiation. Claims about market dynamics, consumer welfare, and competitive effects are pervasive, but empirical support is sparse and contested.*[7]

We emphasise that these criticisms are levelled at all parties to the consultation but that, in our view, **gatekeepers will need to accept a particular responsibility to assist the Commission in its assessment of the impact of the DMA given their role as implementors of the measures the DMA requires and given their ability to provide a wider view of impact than most individual business or end users.** When you are the gatekeeper of a service, you are also the gatekeeper of data related to that service. Although it is possible and to be hoped that the quality of debate improves and matures in subsequent DMA reviews, we think the adversarial nature of the compliance and enforcement processes and the contested nature of objectives do not incentivise any interested party to disclose data inconsistent with their advocacy position. Therefore, we do not expect this data to be forthcoming under the review process (or any other process) without further action by the Commission relying on existing or possibly new legal disclosure obligations.

In addition to this, some reports commissioned by the CCIA have focussed on the impact of the DMA on the implementation costs for gatekeepers or business users[8]. The resulting estimates are highly assumption-driven and present a very wide range of estimates[9]. Such studies provide only a partial

[6] We recognise that some data on the impact of the DMA on use of browsers and search engines has been published by some business users and by some third party analysts, e.g. https://www.reuters.com/technology/eus-new-tech-laws-are-working-small-browsers-gain-market-share-2024-04-10/

[7] https://www.linkedin.com/pulse/dma-article-53-review-mapping-fault-lines-ben-schroeter-n0vke/?trackingId=mkmnmxWJSgir6c0jcCJwYg%3D%3D

[8] Those we are aware of include those by LAMA Economic Research (in conjunction with various authors) at https://www.dmcforum.net/wp-content/uploads/2025/06/120625-FINAL-CCIA-DMA-Report-.pdf and https://ccianet.org/research/reports/costs-to-us-companies-from-eu-digital-services-regulation/

[9] For example, one LAMA study estimates revenue losses for business users of between €8.5 and €114 billion whilst another estimates gatekeeper compliance costs of €1 billion p.a. by extrapolating from claims of resource costs made by an individual gatekeeper.

view of the impact for end users or the market as a whole and surveys of end users undertaken for the CCIA do not appear to us to employ conventional survey standards or methodologies.[10]

We note that BEUC has also provided some high-level indications on DMA impacts on consumer choice (in particular on browsers, third-party apps, payment systems), but without any quantitative evidence or assessment of how end users or business users respond to the presentation of these choices.[11] Some business users have come with more precise data, especially on the positive impact of the DMA choice screen obligations on the take-up of alternative browsers or search engines.[12]

Finally, the **DMA implementation is a very interesting regulatory experiment whose effects are increasingly studied by the academic literature**. As the DMA obligations are unique to the EU and probably one of the most far reaching intervention in digital markets compared to other jurisdictions, the evolution of the EU digital markets and services can be contrasted with the evolution of other markets. The Joint Research Centre of the Commission organised in September 2025, with the Toulouse School of Economics and Yale University, an interesting conference where some papers on the first effects of the DMA obligations were presented.[13] This was followed by a similar conference in February at the University of Georgetown, in cooperation with the Universities of Yale and Princeton.[14]

2.1.2. Commission Annual Reports and Gatekeeper Compliance Reports

The Commission publishes **Annual Reports intended to summarise the Commission's actions to secure implementation and compliance of the DMA, not to assess their impact**. Consistent with this, whilst the Commission's second Annual Report highlights developments such as the availability of new app stores as evidence of the positive impact of the DMA, it does not attempt any kind of quantitative assessment of the impact for end users or business users or the way in which they have responded to the opportunities which the DMA obligations are intended to create.[15]

The **non-confidential versions of compliance reports of gatekeepers similarly lack data on the impact of the obligations** and so, in our view, are unlikely to provide a basis for the assessment which the Commission is expected to undertake under Article 53. Overall, on the basis of these public disclosures, it appears that some gatekeepers engaged more than others with quantitative data and that different approaches have been taken by different gatekeepers. In the absence of greater public disclosure, it is difficult for anybody other than the Commission to assess the relevance or usefulness of the data provided, or what conclusions might be drawn from it.

We recognise, of course, that some of this data may be commercially sensitive for the gatekeeper and that gatekeeper reporting to the Commission may differ from what is provided to the public in the

[10] For example, a survey of end users asking about their online services experiences since 2024 appear to have only included an option to provide responses which were negative, see https://www.nextradegroupllc.com/impact-of-the-dma-on-eu-consumers
[11] https://www.beuc.eu/reports/first-bloom-increased-consumer-choice-after-eighteen-months-dma.
[12] Jesper Akesson, Kush Amlani, Emily Chissell, Robert Hahn, Stefan Hunt, Michael Luca, and Gemma Petrie, An empirical analysis of choice screens, 2026. For a more nuanced view of the effects of choice screen: Omar Vasquez Duque, The Magical Number 2 (Minus Two): An Empirical Analysis on the Efficacy of Choice Screens to Increase Competition in Digital Markets, 2025.
[13] https://www.tse-fr.eu/conferences/2025-economics-digital-markets-act-dma-workshop.
[14] https://kgi.georgetown.edu/events/digital-competition-conference-2026/
[15] https://digital-markets-act.ec.europa.eu/document/download/8ed232e8-a674-4434-a13e-8712ea42b0f5_en?filename=DMA_annual_report_2024.pdf

non-confidential compliance report, including through provision of data in response to other ad hoc information requests from the Commission that we have not seen. It may also be that this data will inform the Commission's assessment of the impact of the DMA in ways that will become clear when the evaluation report is published later in 2026. However, it seems clear from the outputs of the current compliance reporting process that it places limited demands on and provides a large element of discretion to gatekeepers in terms of the data they report. **Without greater clarity of how and what data the Commission requires from gatekeepers, we remain doubtful that these arrangements will allow the Commission to undertake a proper assessment of the impact of the DMA**.

As we discuss further below, the absence of a proper evaluation framework for assessing the impact of the DMA also makes it difficult for either the Commission or any other interested party to determine what data will be required to populate such a framework. We therefore consider that our recommendation that the Commission begin to develop an evaluation framework will also contribute to clarifying the data requirements which we recommend the Commission impose on gatekeepers (and potentially on other parties if necessary).

2.2. Addressing the evidence gap

We have previously proposed that the **Commission should require gatekeepers to measure and report on the impact of implementing different obligations by including a set of 'output indicators' in their annual compliance reports,** as well as publishing these figures on a more regular basis.[16] Our intention was that these indicators would reveal the extent to which end users and business users had engaged with the opportunities that the DMA is intended to introduce and the impact of their doing so. It is important to recall that we drew a clear distinction between 'output indicators' and 'outcome indicators'. The latter refers to the impact of end user interactions on market outcomes such as changes in market shares of different firms, the prices paid by users or the number and quality of the choices they are presented with. These will be the consequence or outcome of user and business user engagement with gatekeepers and gatekeeper responses to that engagement.

We emphasised that we did not presuppose that the effective implementation of the DMA would result in any particular level of user or business user engagement (and so, to repeat, we do not think output indicators should be adopted as 'targets' which effective compliance is expected to achieve) and we said that we expected the outputs to depend upon the context in which particular obligations are being implemented. We provided a list of quantitative measures or indicators to illustrate what we had in mind.[17]

The Commission issued a Compliance Report Template in October 2023, which did include a requirement that reports include

> *'a set of indicators which allow or will allow based on their future evolution the assessment of whether the measures implemented by the Undertaking to ensure compliance are 'effective in achieving the objectives of this Regulation and of the*

[16] https://cerre.eu/wp-content/uploads/2024/01/DMA-Output-Indicators_FINAL.pdf.
[17] The annex appears in the paper cited above.

> *relevant obligation', as required by Article 8 DMA, including an explanation why the Undertaking considers these indicators to be the most suitable'*[18]

and, more specifically,

> *'any relevant data which can inform whether the measure is or will be effective in achieving the objectives of the DMA, such as, depending on the circumstances, data on the evolution of the number of active end users and active business users for the relevant core platform service and, for each relevant obligation, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the number of pre-installed defaults as well as yearly revenues from payments related to those pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc.'.*

However, as already noted above, the non-confidential versions of the compliance reports produced by gatekeepers to date suggest that some gatekeepers have been more responsive to this requirement than others, and it is difficult for us to assess how effective the Template has proven to be in the confidential versions.

Our overall view remains that, **absent a much more explicit and detailed requirement from the Commission, gatekeepers do not have sufficient incentive and so will not voluntarily collect or disclose the quantitative data unless its suits their interests which we think will be required for the Commission to properly assess the impact of the DMA**.

Some gatekeeper interviewees have told us that they did not consider it their responsibility to collect or provide such data to the Commission. Moreover, without such obligations we would expect all interested parties, including but not limited to gatekeepers, to exaggerate the impact of obligations or to offer only a partial assessment of benefits and costs in ways which favour their advocacy positions and in order to influence the Commission's approach to enforcement activity and/or the wider debate about the future evolution of the DMA. This is unavoidable when the process of assessing compliance and the process of assessing impact will be running in parallel to each other rather than in sequence (i.e. with the assessment of impact only following the conclusion of the assessment of compliance).

Our expectations are confirmed by the latest consultation on the DMA evaluation, as well as the other studies that have been published by various interested parties since the DMA was adopted, as discussed above. The public versions of the compliance reports provided by gatekeepers also reveal inconsistent and partial use of output indicators which a more standardised and transparent approach would remove.[19]

Our first recommendation in this paper is therefore to reiterate our previous recommendation that **the Commission require the gatekeepers to provide data against a specified set of output indicators as part of the compliance reporting process**, **but also for the purposes of assessing the impact of the DMA.** We noted in our previous paper on output indicators that Article 21 of the DMA gives the

[18] P. 4-5 at https://digital-markets-act.ec.europa.eu/document/download/904debdf-2eb3-469a-8bbc-e62e5e356fb1_en?filename=Article%2011%20DMA%20-%20Compliance%20Report%20Template%20Form.pdf.

[19] A standardised approach would also allow for the comparison of data from different gatekeepers (in relation to the same obligation and CPS) and aggregation of data, which could improve transparency whilst preserving business secrets.

Commission powers to demand information from any undertaking for the purposes of undertaking its duties under the DMA. This would include an assessment of its impact as required by Article 53 as well as an assessment of compliance and implementation for the purposes of Article 35. We think our proposals in relation to output indicators could play an important role in both contexts.

It is important to recognise that implementing this recommendation involves risks for both gatekeepers and the Commission itself, since neither will be able to anticipate the outputs of any assessment which the data is intended to inform. In this sense, **all parties will need to commit to a process without knowing the outcome in advance**. If the Commission were to implement our recommendations, it may find itself having to concede that certain aspects of the DMA have not been beneficial for business users or end users, or have otherwise imposed a disproportionate burden on them. Gatekeepers may find that the Commission is able to demonstrate, with rigorous evidence, that particular obligations have been highly beneficial for end users. However, the process we envisage will require all sides to commit to developing a proper, evidence-based evaluation framework which would be used to inform how the DMA evolves. In making this recommendation, we also hope that all sides in the public debate about the DMA move beyond the narrow question of compliance (important though that remains) and to a discussion of the impact of the DMA (and potential changes to it) that is informed by robust data and a proper evaluation framework.

Some related actions may complement this recommendation. For example, the **Commission has begun to provide information about the opportunities that are available for business users as a result of the implementation of the DMA**. On its website, there is a page dedicated to "Resources for Businesses" which allows business users to see quickly what options each gatekeeper has.[20] This is similar in spirit to our recommendation that gatekeepers provide 'dynamic' compliance reports which are constantly updated, rather than static reporting.[21] On this page, the business user can access the most up-to-date information about how to take advantage of the DMA. For interoperability, a quick factsheet has been designed to introduce business users to how they can take advantage of the new specification decisions.[22] We think these steps may be helpful in increasing awareness of the opportunities created by the DMA and can contribute to the achievement of the DMA objectives (although again a proper framework is first required before that assessment could be made). Later in this paper we suggest that similar actions may be required to ensure that end users can benefit fully from the opportunities created by the DMA, particularly when users are being invited to choose between competing products.

Finally, the Commission could collect and summarise in **one public repository all academic research** done on the impact of the DMA, including those already mentioned above.[23] This academic research could be vastly expanded if the **DMA** would allow **independent and vetted researchers to have access to all the data necessary to monitor the compliance by the gatekeepers with the DMA obligations**, as it is already foreseen for the DSA with the famous **Article 40.**

[20] https://digital-markets-act.ec.europa.eu/questions-and-answers/resources-businesses_en.
[21] De Streel et al, The DMA@1.
[22] https://digital-markets-act.ec.europa.eu/questions-and-answers/interoperability_en.
[23] See footnotes 14 and 15.

3. Developing a robust evaluation framework

Beyond addressing the evidence gap, a related and more fundamental challenge is the development of a robust framework to evaluate the positive and the negative impact of the DMA. While the Commission has, at least in principle, articulated sound ex post evaluation standards in its Better Regulation Guidelines,[24] recent studies suggest that these principles are not consistently applied in practice across EU policymaking,[25] including in the digital domain. [26]

The Commission's evaluation of the GDPR illustrates this. In 2020, only two years after the Regulation became applicable, the Commission published a first evaluation report that contained no quantitative assessment and relied largely on broad political narratives, emphasising citizen empowerment, values-based innovation, and internal market objectives.[27] While the absence of quantitative analysis may partly be explained by the limited time elapsed since implementation, the report also failed to establish an evidence-based evaluation framework or to identify the key indicators and data that would need to be collected for a meaningful assessment over time. The subsequent evaluation report published in 2024 was similarly limited, again largely reiterating high-level political messaging rather than providing a systematic assessment of impacts.[28] This is particularly striking given that, only weeks after the Commission's report, the Draghi report referenced several academic studies offering quantitative evidence on the effects of the GDPR, notably with respect to innovation.[29]

3.1. The timing of the evaluation

There are **at least three reasons why the impact of the DMA cannot be assessed completely and immediately** and why, therefore, the forthcoming 2026 evaluation should be viewed as the start of a longer process which will continue over several review periods.

A first reason is that the **compliance process under the DMA continues to be an iterative process**. Therefore, any definitive assessment of the impact of the DMA from which robust conclusions might be drawn will have to wait until the iteration has largely been completed and effective compliance achieved, or at least until it has progressed further than is the case today. This is not to say that provisional assessments should not be undertaken in the meantime and would not have an important purpose, as discussed further below.

A second reason for delaying any assessment of impact is that **end-users' and business users' responses to the opportunities created by the DMA are likely to take some time to occur fully and so the impact on business or end user behaviour is likely to develop over time**. On the business user side, the iterative process described above may delay decisions to launch new services which depend upon a stable set of processes and specifications from the gatekeeper or may mean that services which

[24] Commission Better Regulation Guidelines of 3 November 2021, SWD(2021)305, Chapter 3.
[25] A. Bucher and E. Golberg, Better regulation in the European Union needs a fresh start, *Bruegel Policy Brief* 01/2026.
[26] M. Bassini, M. Maggiolino and A. de Streel, Better Regulation and Evaluation for the EU Digital Rulebook, CERRE Report, Jan 2025, pp.36-41.
[27] Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM(2020) 264 and SWD(2020) 115.
[28] Second Report on the application of the General Data Protection Regulation, COM(2024) 357.
[29] Draghi Report, Part B, p.319.

are launched do not get the response from end users which they would obtain under conditions of effective compliance.

On the end user side, the DMA is being introduced into markets in which end users have already acquired deeply embedded habits in terms of how they choose and interact with different core platform services. One interviewee noted that the DMA requires gatekeepers to introduce measures which in some cases will force end users to alter these habits, for example by actively selecting from a choice screen rather than relying upon defaults or actively choosing their preferred services through other means.[30] End-user responses will of course also differ depending on the context and individual preferences and it is unclear at this stage the what extent the DMA will drive changes in how end users engage with digital services, or what the aggregate effect of this will be.[31] It is also likely that habits will take time to change, given consumer inertia and risk aversion, as shown by experience from other markets, such as utilities. Digital markets may be particularly challenging because many services are provided without a price for the user, meaning that competition between suppliers is likely to focus on non-price aspects of the services which may be more difficult for users to assess or respond to. To be clear, we consider that end users can generally be expected to benefit from having choices but that it will take time for them to respond and for these benefits to be realised.

Thirdly, **the Commission will first need to develop a comprehensive framework for assessing the impact of the DMA**. As will be clear from the discussion earlier in the paper, we do not consider it or anyone else has that framework today and an important aim of this paper is to show what that framework might consist of in anticipation of the Commission committing to develop it for the future.

3.2. A cost-benefit framework

Therefore, we think that the Commission should use the opportunity of the 2026 evaluation to build a robust evaluation framework (and take steps to assemble and collect the data to populate it, as discussed in the previous section) to assess whether the DMA is meeting its objectives of contestability, fairness and delivering a single internal market, but also whether it is contributing to innovation and user choices. As it develops this framework, the Commission should consult with the national regulators and the interested parties, including gatekeepers, business users and civil society groups. Then, the publication of the second Review report by 2029 ought to provide a first opportunity to use the framework to assess the impact of the DMA. At that stage we hope that compliance should be substantially achieved, although we expect that further refinements to compliance practices would continue to be made after that.

The Commission services' **impact assessment** of 2020 for the DMA proposal listed a number of benefits and costs which are well summarised in the opinion of the Regulatory Scrutiny Board.[32] The expected benefits were the following:

[30] Hunt Allcott, Juan Camilo Castillo, Matthew Gentzkow, Leon Musolff, and Tobias Salz, Sources of Market Power in Web Search: Evidence from a Field Experiment, NBER Working Paper 33410, 2025.
[31] In making this point we do not presuppose that all or even many end users will necessarily exercise choices more frequently as time advances. We are simply saying that the impact of any measures taken by the gatekeeper, in terms of changes in end user behaviour, may take time to become fully clear.
[32] Impact Assessment Report of the Commission Services of 15 December 2020 on the Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363.

1. Reduction of *market concentration* due to decreased entry barriers: a decrease in the Herfindahl-Hirschman Index (HHI) by 0.25 (for user share) and 0.11 (for revenue share);
2. Increase in *R&D investment* due to market de-concentration and resource reallocation from mergers and acquisitions (M&A) to R&D: €12-23 billion.
3. Increase in *innovation* due to higher R&D investment: €221-323 billion.
4. *Economic growth* resulting from increased R&D in the ICT sector: €12-23 billion.
5. Reduction in *internal market* fragmentation, which would foster increased online cross-border trade and its indirect/spillover effects: €92.8 billion.
6. Overall increase in *consumer surplus* from lower costs and prices, as companies could reduce spending on online ads: €13 billion.

The expected costs had a range from €43.8 million to €50.9 million, covering the following components: [33]

- *European Commission*: implementation and supervision costs of €16.7 million (80 FTEs, IT support, and external expertise).
- *National authorities*: €6 million (based on 3.5 FTEs for 27 Member States).
- *Gatekeepers*: €21.15 million for 15 designated gatekeepers.
- *Business users*: net additional resource requirements are expected to be very limited, as costs associated with legal actions against gatekeepers under other EU or national laws (e.g., competition law) would be redirected to DMA enforcement actions.

However, the categories of benefits were defined at a very general level, and the quantitative estimates covered a wide range. The underlying methodologies and their limitations were not always sufficiently explained, as outlined by the Regulatory Scrutiny Board. Moreover, the cost assessments focused primarily on administrative compliance and supervision costs, overlooking other potentially significant cost components, and appear to have been underestimated as the current staff in the gatekeepers and the Commission for the compliance and supervision seem to exceed what was foreseen in the impact assessment. Therefore, in light of the lessons emerging from the first years of DMA implementation, a significantly more robust and disaggregated evaluation framework should be developed, commensurate with the DMA's importance for the regulation of the EU platform economy.

This evaluation framework should **identify and compare all the relevant benefits or impacts of applying an obligation to a particular core platform service against all the relevant costs of doing so**.[34] Ultimately, we think that the assessment should relate to the costs incurred by end users,

[33] The projected costs and benefits are summarised in the Regulatory Scrutiny Board Opinion of 10 December 2024 on the DMA draft Impact Assessment.
[34] Some of these costs will have already been sunk by gatekeepers when taking steps to comply with the obligation at the outset, or through subsequent iterations. These costs are largely irrecoverable now and should not in our view feature in the assessment. However, there are other forward-looking costs which ought to be considered, some of which are incurred directly by the gatekeeper, some by business users and some by end users.

recognising that costs which are incurred by firms may be passed on to end users in some form and to some extent (although not always in the same digital market in which they were incurred).[35]

The **categories of benefits** arising from the DMA and to be included in the framework would include:[36]

Potential end-user benefits from innovation, quality, or price benefits resulting from:

the entry of new third-party (or improvements) in existing services that complement the core platform services;[37]

the entry of new third-party services that compete directly with core platform services.[38] The Commission highlights the entry of three new app stores – Epic, Aptoide and AltStore – as evidence of the impact of these provisions in the second Annual report.[39] These new entrants are able to offer differentiated products, competing by providing other services (e.g., providing specialised gaming only stores with a wider choice of games than those on rival app stores or better privacy settings). We have also seen increased take-up of new browsers and search engines, which differentiate their services from those of gatekeepers. These benefits would include improvements in the quality of gatekeeper services in response to entry;

the improved performance of gatekeeper services that arise in response to inter-platform competition from third parties or because the DMA stimulates competition between gatekeepers, including because gatekeepers develop services in the future which already anticipate compliance with the DMA. These benefits also arise from the mere threat of competition because markets are contestable and entry barriers have been reduced thanks to the DMA;

Potentially lower costs for end-users from switching between services or between core platform services;[40]

Potential privacy benefits for end-users arising from measures which allow user to withhold consent to the sharing and processing of personal data (and thereby avoiding personalised advertising) whilst retaining access to a core platform service,[41] but also resulting from the entry of new core platform services which differentiate themselves by offering greater user privacy;[42]

Potential business user benefits that arise from more effective or lower cost advertising or transaction services on the core platform service or on third-party platforms[43] or from better

[35] This point is important to counter claims that the DMA is intended to favour the interests of particular firms, notably European firms, to the detriment of European users.
[36] This list is intended to be illustrative not exhaustive.
[37] Likely to result from the implementation of Articles 5.3, 5.4, 5.5, 5.7, 6.3, 6.4, 6.7, 6.10 and 6.12 DMA.
[38] Likely the result of the implementation of Articles 5.8, 6.2, 6.3, 6.5, 6.10 and 6.11 DMA.
[39] Op cit para 45.
[40] Likely the result of the implementation of Articles 6.3, 6.6, 6.9 and 6.13 DMA.
[41] Likely the result of Article 5.2 DMA.
[42] E.g., DuckDuck go martes itself as offering a browser that 'actively protects your personal information' https://duckduckgo.com/.
[43] Likely the result of Articles 5.9 and 6.8 DMA.

terms of trade with the core platform service gatekeeper.[44] Business users may be able to switch core platform service providers, or to multi-home and encourage gatekeepers to improve their terms of trade;

Potential benefits to society as a whole from disruptive innovation, for example intermediary services could be offered to stimulate some of the DMA entitlements, for example actors that help end-users take advantage of data portability.[45] These actors may include gatekeepers entering new markets.[46]

Similarly, the **categories of costs** to be assessed would include:

Ongoing compliance costs incurred by the gatekeeper (such as legal and administrative costs) *and opportunity costs* if engineering and other resources are diverted to maintaining compliance.[47] Compliance costs are inherent in most regulatory regimes and so our point here is to highlight that these costs should be assessed alongside the benefits of DMA compliance and one should be sensitive to settings where the marginal cost of compliance vastly exceeds the benefits;[48]

Innovation losses if gatekeepers withhold permanently (or for a long period) and modify new services (in ways which are detrimental to end users) or are less incentivised to innovate in the EU because they are required by the DMA to first take additional steps to enable third-party access or other measures. Assessing these losses will be challenging and their impact may depend upon the extent to which a gatekeeper acts as a first mover or a follower in introducing new services, as compared to third-party providers or other gatekeepers who the DMA may enable to act as first movers.[49] It may also be difficult to assess whether modified services are of inferior quality to those offered in other jurisdictions where the DMA obligations do not apply, or how significant any differences actually are. The Commission will likely require evidence from the gatekeeper to undertake this assessment, recognising that gatekeepers may also be in a position to influence the evidence itself (see below);

Losses in differentiation between core platform services which compete with each other, and which have been discussed above. As we explained in the next sub-section 3.3., the impact will vary between different groups of users depending upon their preferences and may be offset by the availability of differentiated third-party offers. Some users may experience this as a reduction in quality (for example, if compliance with the DMA adversely impacts privacy or security features), others may benefit from it if it means they consider certain services to be better and closer substitutes than before;

[44] Likely the result of Article 6.12 DMA.
[45] E.g., the Data Transfer Initiative https://dtinit.org/.
[46] E.g., data portability solutions offered by Microsoft Fabric.
[47] This should exclude any costs incurred to comply with legal obligations established by proceedings outside the EU (but which may also contribute to compliance within the EU).
[48] Studies we have seen to date tend not to distinguish between sunk or non-recurring costs and ongoing costs. We think only the latter should be included in the assessment.
[49] Another concern was raised by one interviewee that had been designated a gatekeeper on an EU-wide basis but argued that e-commerce markets were national in scope and that it was a challenger in a number of national markets. It said it was required to comply with the DMA obligations irrespective of its position at national level, and that this (unfairly) inhibited its ability to compete in those markets where it was a challenger.

Potential losses suffered by business users as a result of the DMA, whilst acknowledging that business users also potentially benefit from greater competition in the provision of core platform services or related services or from terms of trade with the gatekeeper that are fairer than pre-DMA or services that are more responsive to their requirements (e.g. as a result of greater engagement between gatekeepers and business users)[50].

One cost highlighted by some gatekeepers is a *reduction in the capacity to engage in personalised or targeted advertising* via the core platform service, given obligations which restrict the capacity of gatekeepers to combine or acquire personalised data from end users at whom those adverts are targeted. Whether and to what extent a reduction of the personalisation of advertising will represent a detriment to end users is a complex matter, since it will depend upon how different business users and different end users respond, meaning there will be complex second order effects;

Another cost could arise if greater inter-platform competition means that *app developers or other business users have to develop multiple different versions* of their product to reach end users;

A further example, cited earlier, arises if particular measures *benefit some users at the expense of others*. In the example cited, direct suppliers may face financial costs in reaching end users which they have previously been able to avoid.

End users may incur direct costs in terms of:

time and effort required to navigate choices which have not previously been presented to them (the most obvious being the obligation on gatekeepers under Article 6.3 to introduce choice screens before users select browsers, search engines or virtual assistants), although it may be reasonable to assume that users will invest effort in proportion to the benefits they might perceive from doing so.

lower quality of the gatekeeper's services as a result of the obligations, for example because services have become less integrated[51] or more vulnerable to cyberattacks[52] or are less privacy preserving. However, those costs depend on the compliance path chosen by the gatekeeper. They may be offset to a greater or lesser degree by other DMA obligations which reduce switching costs. As noted earlier, we think the key point is that user preferences and user capabilities will differ, so that measures which represent a significant cost for some users may not be significant for others. There is of course no reason to think that the relative size of benefits and costs for individual users will be correlated, and it appears more likely that users who might be expected

[50] In principle business users (unlike gatekeepers) are free to avoid these costs and so it is reasonable to assume that in the long run they will only engage with Core Platform Services if it is in their interest to do so. However, poor or slow enforcement of the DMA may result in business users incurring costs which exceed their expectations, or which they have to write off if they subsequently decide to exit. These should be taken into account in the assessment.

[51] Louis-Daniel Pape, Michelangelo Rossi, Is Competition Only One Click Away? The Digital Markets Act Impact on Google Maps, CESIfo Working Paper 11 226, 2026.

[52] Gatekeepers may take steps to mitigate these costs by, for example, delaying the introduction of services until the security concerns can be addressed. Output indicators could be developed to assess the impact of DMA obligations upon the security of services provided by the gatekeeper (and potentially by third parties).

> to derive limited benefit from the DMA measures may also be those who incur the greatest costs. The overall impact for users cannot be predicted in advance or without a detailed assessment.

We recognise that gatekeepers may have both an ability and incentive to incur costs or to impose costs on business users and/or end users in order to influence the assessment which we recommend the Commission undertakes. Our recommendations on output indicators relate predominantly to data which would inform an assessment of the benefits of implementing a DMA obligation rather than the costs, but we suggest that the Commission take a similar approach in requesting data pertaining to costs in a similar standardised format from all gatekeepers. **This would enable the Commission to benchmark data on costs as part of an assessment of whether a particular set of costs should be attributed to compliance with the DMA or be excluded from the assessment on the basis that they were incurred unnecessarily or with the intention of circumventing or delaying compliance**. This will be a challenging exercise, but the Commission's views as to which costs can legitimately be attributed to complying with the DMA and which are attributable to inappropriate strategic behaviour will no doubt also be informed by the experience of engaging with the gatekeeper in question throughout the implementation process[53].

We expect **some benefits to take time to be realised**, even after effective compliance has been achieved, for the reasons already discussed in this paper. It may be easier to identify costs of compliance in the short term, although this is itself challenging as the direct costs incurred by gatekeepers are difficult to verify and represent only one aspect of the costs that need to be taken into account. The studies undertaken to date and the various public claims made by gatekeepers, illustrate these challenges.[54]

The evaluation framework based on a cost-benefit analysis **could ensure that the DMA as a whole becomes, over time, an instrument which is more effective and more proportionate and tailored to the different business models of the gatekeepers and that is applied where the beneficial impact of the measures can be shown to have outweighed the corresponding costs.** It will also allow the Commission to begin to identify, on the one hand, the DMA obligations which have the most beneficial effects and whose enforcement could be prioritised and, on the other hand, obligations that, when applied by particular gatekeepers to certain core platform services, have little or no discernible impact but involve significant implementation costs.[55] This is particularly important for the DMA which imposes a common set of obligations upon a wide variety of different firms and services.[56] Because of its one-size-fits-all approach, the impact of the DMA is likely to be more significant in some contexts

[53] We note that, in principle, similar considerations apply to an assessment of the benefits if a gatekeeper is judged to be compliant but the Commission considers that it has been able to implement measures in way which minimises the beneficial impact. These assessments are very difficult because they cannot be informed by data and so will require a degree of speculation on the Commission's part. Our recommendation would be that the Commission's assessment relies upon the data provided by the gatekeeper (and other sources) to the Commission, but that the interpretation of the results is done with these considerations in mind.

54 See footote 9.

[55] For instance, an interviewee has suggested, for example, that allowing end users to port their e-commerce shopping data under Article 6.9 has had no impact because there is no demand from either business users or end users to port data in this particular context. This is contrasted with other Core Platform Service, where the porting of data may have a greater impact. Obviously one interviewee is not enough to draw solid conclusions and the Commission says in its second Compliance Report that all gatekeepers have implemented the portability measures and that it will 'monitor the functioning of these new tools.': Para 31 at https://digital-markets-act.ec.europa.eu/document/download/8ed232e8-a674-4434-a13e-8712ea42b0f5_en?filename=DMA_annual_report_2024.pdf.

[56] This one-size fit all has been criticised in the literature: https://cepr.org/voxeu/columns/european-commission-digital-markets-act-translation?s=09#.X_S5Rss3Eks.twitter

than others. It may be positive in some contexts but neutral or even negative in others. A nuanced and subtle approach will be required to assess this.

3.3. Differentiated Services and Heterogeneous Users

One aspect of the impact of the DMA that arose during our interviews was that whilst the impact of some DMA obligations will be to enable new forms of competition, other **obligations are being applied to core platform services where a degree of differentiated competition between gatekeepers already exists.**[57]

Our starting point is that **the capacity to differentiate is an important feature of competition and driver of innovation in digital markets which should not be unduly compromised by the DMA**. This does not mean we would uncritically accept claims that any loss of differentiation is to the detriment of users (or even that such differentiation always exists[58]). Any loss of an individual gatekeeper's capacity to differentiate should be assessed against any positive impact arising from third parties who are able to take advantage of the opportunities provided by the DMA and offer services of their own in competition to the gatekeeper. It may also be that some forms of differentiation are not greatly valued by some users or may even disadvantage some of them (as when they contribute to switching costs) while being valued by others. The DMA might also result in greater differentiation and choice for services in some digital markets (e.g. through entry), even if this could be accompanied by some loss of differentiation in other markets.[59]

These observations apply not only to the impact of the DMA on end users of differentiated services supplied by different gatekeepers but also to the impact on end users of an individual gatekeeper. Some users of the services of that gatekeeper may value the opportunity to use a different app store, browsers or search engines, but others may not. Users are also likely to differ in their capacity and willingness to take advantage of the opportunities presented to them, as some may find it more difficult to navigate choice screens or to engage inside loading apps than others (although, as noted earlier, some end users may learn or otherwise change their habits over time).

This has at least two consequences for assessing the impact of the DMA. First, **claims that all end users are unambiguously harmed or unambiguously benefit from the implementation of particular obligations are likely to be implausible**. The situation will invariably be more nuanced when any given measure is likely to benefit some users and inconvenience others, and likely to different degrees

[57] The obvious example is competition between Google/Android and Apple/iOS for the mobile operating systems, being mass market services for which there is demand from a very wide range of business and end users. Evidence of end users of different services having different preferences is presented in chapter 6 of the CMA's Strategic Market Status Investigation into Google's Mobile Platform, esp. para 6.15, at https://assets.publishing.service.gov.uk/media/68f8bf4780cf98c6e8ed8f83/Final_decision_report.pdf. We are not making any assessment about the strength of the competitive constraints or degree of market power associated with such differentiation, only that there is evidence of heterogeneous demand.

[58] There is room for debate about whether claims of service differentiation (e.g. with respect to security or privacy) are accurate, but even if they are not, users may perceive such differences to exist and respond on that basis. One of the recommendations we make below is that the Commission consider ways in which end users might better understand the actual, as opposed to perceived, differences in the services offered by different gatekeepers.

[59] As an hypothetical example: (i) the existing users of a mobile ecosystem who prefer existing services of that ecosystem and do not value the opportunity to use third party services may lose; (ii) existing users of that ecosystem who prefer some services of that ecosystem but who may value other third party services which they were unable to access pre-DMA may lose or may benefit; (iii) the users of a mobile ecosystem who value third party services which they were only able to access on this ecosystem devices pre-DMA, or were not able to access at all, may benefit if they are now able to switch ecosystem without forgoing those services.

between different gatekeepers. The task is therefore to quantify the relative magnitude of these different effects using robust empirical evidence. As part of its work on developing an evaluation framework, the Commission will need to consider how this is to be done (likely including through the use of user surveys).

Second, given such differences in preferences, **there is no reason to expect that the response of users of core platforms which are differentiated (e.g. mobile operating systems), would necessarily be the same even if the measures being taken by each gatekeeper to comply with the DMA were to be identical.** That is because the preferences of the end users themselves, and the way they assess opportunities provided by the DMA, will not be homogeneous. This means that any attempt to benchmark or otherwise compare the outputs when different gatekeepers implement the same obligations in respect of the same core platform services (as we advocated in our earlier paper on output indicators) needs to be approached with a degree of caution, which is not to say that it might not still be useful and informative to do. We should not necessarily expect the impact of an obligation to be the same for different gatekeepers in the presence of differentiated services and different end user preferences, and so the impact of effective compliance by one gatekeeper differ from the impact of effective compliance by another.[60]

Differentiation may also be relevant when assessing switching by end users between two existing but differentiated core platform services. Low levels of switching might indicate that preferences are widely dispersed and that the two services appeal to different types of users. But it might also indicate that the services are close substitutes for many users but switching costs are too high for most users. Some obligations, such as Article 6(9), are intended to reduce those switching costs and, as noted earlier, for others it may take time for end users to learn to engage effectively with the opportunities which the DMA is intended to ensure are presented to them. Again, we emphasise that there is no 'target' level of switching (or any other output indicator) to indicate compliance or non-compliance but **our point here is also that differences in the level of switching undertaken by customers of different gatekeepers is to be expected in a differentiated service market and those differences may therefore be evidence of different user preferences rather than different levels of compliance**.

Taking these points together, our recommendation is that the Commission should take differentiation seriously and aim to **avoid regulatory solutions that, on the one hand, unnecessarily reduce opportunities for gatekeepers to differentiate their core platform services. On the other hand, the Commission should promote solutions that stimulate user understanding of differences between different services and allow users to exercise choices in light of that**. This raises questions about how the Commission might ensure that, having introduced new choices, end users are then able to effectively engage with the opportunities which the market provides. The DMA aims to alter the supply side of a wide range of digital markets, but there may in future be a need to focus also on the demand side to ensure that end users better understand the choices that are available to them.

[60] We recognise that if the Commission is unable to benchmark outputs for different gatekeepers implementing the same obligations for the same CPS (or should at least interpret such exercises with caution) then it becomes more difficult to assess compliance since the Commission will need to find a 'compliant' counterfactual against which to compare the performance of the gatekeeper in question, particularly as we have said we do not regard output indicators as targets to be met. As already noted, the challenge of defining what a 'compliant' counterfactual looks like lies at the heart of many gatekeeper complaints about a lack of clarity over the measures they are required to take. To be clear, we are not suggesting that different gatekeepers should be held to different standards of compliance, but that the impact of holding different gatekeepers to the same standard may differ. The question is to what extent since significant differences in output indicators may be evidence of different user preferences or evidence of differences in the level of compliance.

4. Improving DMA Impact

One important way to increase the DMA's impact is to ensure that gatekeepers fully comply with their obligations and this is what the Commission has rightly prioritised. But we don't analyse compliance in this report. Compliance may be facilitated and impact may be increased with some improvement on implementation such as: (i) the Commission should continue its efforts to enhance legal predictability and base its prioritisation strategy on a structured cost-benefit analysis; (ii) regulatory coherence across DMA obligations should be improved; and (iii) insights from international antitrust and regulatory experience, including from jurisdictions outside the EU, should be systematically taken into account.

4.1. Improving Legal Predictability and Prioritisation

We explained in the CERRE report on the DMA last year that the **compliance process under the DMA was an 'iterative process'**.[61] The Commission's second Annual Report emphasises the ongoing or incomplete nature of this process, stating that the Commission is 'continuing to collect market feedback on whether the implemented solutions are effective'[62], is 'monitoring these developments'[63] or 'still in the process of assessing compliance.'[64] Thus the iterative process has continued, which is confirmed by the stakeholders we interviewed this year. A feature of the way in which the Commission has chosen to enforce the DMA has been to provide informal feedback to gatekeepers, generally in private, on the extent to which existing measures they have taken or may be contemplating are considered to fall short of 'effective compliance', often having previously consulted with third parties or received various representations from them.

On the one hand, some business users we have interviewed continue to complain that some DMA obligations which are very clear and self-enforcing have not yet been fully applied by some gatekeepers. Moreover, they explain that sometimes the Commission gives them little feedback on the contribution they bring to the Commission.

On the other hand, some gatekeepers we have interviewed continue to complain that the Commission has not provided them with clear instructions as to what measures would constitute 'effective compliance', although we note that gatekeepers continue to appear reluctant to seek clarity from the Commission by requesting a specification decision, as envisaged by Article 8 of the DMA.[65] Some gatekeepers also told us that even if the Commission is not providing feedback that suggests further steps are required, the Commission will not affirmatively state that a gatekeeper is now regarded as being in effective compliance; although others have suggested that the Commission's decision to close enforcement proceedings against Apple in relation to Article 6(3) in June 2025 could be viewed as an example of the Commission indicating that it considers Apple to be in compliance.[66] In most cases the

[61] R. Feasey, G. Monti, A. de Streel, *DMA@1: Looking Back and Ahead*, CERRE Book, March 2025.
[62] In relation to Article 6.9, p.7 at https://digital-markets-act.ec.europa.eu/document/download/8ed232e8-a674-4434-a13e-8712ea42b0f5_en?filename=DMA_annual_report_2024.pdf.
[63] In relation to Article 7, op cit p.8.
[64] In relation to Article 6.11, op cit p.9.
[65] This issue is a recurring theme in our interviews with both gatekeepers and business users. In our view it reflects the difficulty in defining an 'effectively compliant counterfactual' against which the Commission can then assess the actions being taken by the gatekeeper.
[66] https://ec.europa.eu/competition/digital_markets_act/cases/202525/DMA_100185_1229.pdf.

gatekeeper seems to be invited to infer that the absence of any enforcement action by the Commission could be regarded, according to the general principle of legitimate expectations, as good compliance.

We agree with interviewees that the **Commission should provide greater clarity and certainty on the interpretation of DMA obligations** and ultimately, as to what is required of gatekeepers and the opportunities expected for business users and end users. The ultimate interpreter of the DMA is obviously the Court of Justice of the EU, but legal clarifications by the Commission may increase legal predictability and therefore the impact of the DMA. Informed by the better evidence-based and evaluation framework we are calling in the previous sections, those legal interpretations should ensure an effective and proportionate implementation of the DMA.

The Commission has already several legal means to provide those clarifications through hard law instruments such as the **specification decisions** which clearly indicate how the gatekeeper should comply with a DMA obligation or **the non-compliance decisions.** The Commission could also rely more on soft law instruments such as **guidelines.**[67] As we note in the companion issue paper on the regulatory interplay, those guidelines could clarify that aligning with pre-set Commission guidance on specific elements of the DMA's obligations would imply compliance, thereby shifting the burden of proof away from the gatekeepers.

For the future and in the context of the DMA review, a formal process, akin to the **provision by the Commission of individual 'comfort letters' or collective block exemption Regulation** in antitrust cases could be introduced. Moreover, some obligations could be clarified in the light of the two first years of implementation through Commission **delegated acts** under Article 12 of the DMA.

We also think that the **Commission's prioritisation strategy could be clearer and based on structured cost-benefit analysis** informed by the evidence-based and evaluation framework we are calling in the previous sections. Such an approach would ensure that enforcement efforts are proportionate, efficient, and targeted towards areas where interventions are likely to generate the greatest positive impact on market contestability and fairness.

4.2. Improving Coherence Across Obligations

The aim of the DMA is to promote contestability and fairness in digital markets and effective compliance by gatekeepers with the full range of obligations is intended to achieve this. As the impact of these compliance efforts becomes more apparent and better understood, we recommend that the **Commission aims to ensure that the various incentives or opportunities which different obligations may introduce work together in a coherent and aligned manner rather than in conflict or contradiction with each other.** Where there is a tension between obligations, the Commission should resolve it.[68]

[67] For instance, the joint Commission-EDPB draft guidelines of October 2025 on the interplay between DMA and GDPR.
[68] In this section, we deal with the regulatory coherence among the obligations within the DMA. In the companion issue paper on regulatory interplays, we deal with regulatory coherence across among the DMA and other EU regulatory instruments.

Consider, for example, **obligations relating to apps and app stores**. In its second Annual Report on the DMA, the Commission highlights the arrival of three new app stores as evidence of the DMA's market impact. There are a number of obligations which address app stores:

- Article 5(4) DMA allows app developers to steer end-users that have been acquired through the gatekeeper to make transactions (including payments) through a third-party or website;
- Article 5(5) DMA ensures that the content and services purchased in a third-party applications store will function on the core platform service;
- Article 5(7) DMA ensures that developers can use the gatekeeper applications store whilst at the same time using third-party payment services;
- Article 5(8) DMA prohibits tying of the gatekeeper app store with other core platform services;
- Article 6(3) DMA allows the user to uninstall the gatekeeper applications store;
- Article 6(4) DMA allows users to sideload a third-party applications store and to set it as their default store; and
- Article 6(12) DMA requires gatekeepers to provide access to app stores on FRAND terms.

In regulatory matters there is often a distinction drawn between the promotion of inter-platform competition and intra-platform competition.[69] Applied to app stores, the former approach would assume that the core platform service can be fully or partially replicated so that there will be direct competition between two or more independent app stores. The terms on which app developers deal with gatekeeper app stores will then be disciplined by the threat of developers or end users switching to another app store or multi-homing across several applications stores. In contrast, measures to promote intra-platform competition are based on the assumption that the core platform service cannot be fully replicated, and so the best interventions will be aimed at making the terms of access to the gatekeeper app stores more fair, but that competition can be introduced in markets such as for payment services that sit downstream of the gatekeeper applications store.[70]

If we use this framework to analyse the obligations in the DMA that apply to applications stores, **most articles (5(5), 5(8), 6(3) DMA) appear intended to promote *inter-platform competition*** between competing applications stores. However, this intention is not clear as, for instance, there are no obligations to remove the default settings or preinstallation of applications stores on devices (since the provisions to introduce choice screens in Article 6.3 do not apply to applications stores) which could also promote inter-platform competition.

Other obligations, such as Article 5(4) (for payment services), 5(7) and especially 6(12) DMA, appear more likely to promote *intra-platform competition* by directly improving the terms under which app developers can use the gatekeeper applications store. The effect of implementing these obligations is likely to be to make the gatekeeper app store relatively more attractive to app developers (as compared to the position absent the DMA) and to make applications stores in general a less profitable

[69] M. Armstrong, Competition in Two-Sided Markets, *RAND Journal of Economics* 37(3), 2006, 668-691; C. Wang and J. Wright, Regulating Platform Fees, *Journal of the European Economic Association*, 23(2) 2025, 746–783.

[70] A similar point is made in the LAMA Economics report: 'An evaluation of the rationale for the platform organisation and of the benefits they generate is probably needed for a careful implementation of the DMA. In some instances, promoting platform differentiation and inter-platform competition might be a more efficient solution to the problem of entry and choice.', see p.7 at https://www.dmcforum.net/wp-content/uploads/2025/06/120625-FINAL-CCIA-DMA-Report-.pdf.

business (assuming that the FRAND obligations of Article 6(12) have the effect of reducing the level of fees payable by developers to the gatekeeper app stores and, thereby, the profitability of that app store and any other app store that would compete with it). These impacts are likely to discourage entry and investment by third-party applications store providers and so weaken the prospects for the inter-platform competition. Thus, measures to promote intra-platform competition may undermine the effectiveness of other measures that are intended to promote inter-platform competition.

We recognise that the Commission may wish to hedge its bets and simultaneously pursue both approaches to competition, accepting the inherent tensions in doing so which we have described above. Other regulators faced with similar dilemmas have taken a similar 'hedging' approach, although experience suggests that regulation is much more effective when all the incentives are aligned.[71] One way is to approach the regulatory problem dynamically and pursue first the intra-platform competition, which is easier to achieve and then, the inter-platform competition which is most powerful.[72]

In addition to this, fairer terms from the gatekeeper app store may mean that app developers lose the incentive to develop apps that may be used on the web without downloading these from any applications store, whether gatekeeper or third-party. The use of such progressive web apps is also supported by the DMA and could be an alternative way of stimulating competition by providing substitutes to app stores. It is only as the DMA is implemented and the impacts can be assessed that the merits of one approach over another may become apparent.[73]

We are not recommending at this stage that the Commission favour one approach over another, but it is important to recognise the tensions between different obligations when they arise, each of which may be legitimate in itself and may address the concerns of a particular constituency. Since most obligations were adopted in light of previous antitrust complaints or cases relating to gatekeeper conduct in digital markets and different complainants may have different objectives, it is perhaps not surprising that these tensions arise. In the longer term, we think the DMA will be more effective and have a greater impact if the Commission aims to resolve these tensions and clarify its objectives. This will likely mean the Commission withdrawing measures which work against the form of competition or contestability it is seeking to promote. It may also mean supplementing existing obligations with other measures (e.g. extending Article 6(3) to app stores) to ensure they are fully effective. Providing this clarity may assist gatekeepers in their efforts to comply with obligations and may also assist prospective entrants (who may otherwise be unsure about which form of competition the Commission is prioritising).

[71] An example is the long-standing debate in Europe about inter-platform vs intra-platform competition in telecommunications markets. For many years the European Commission and national regulators sought to calibrate regulated access prices in order both to encourage entry and investment in network infrastructure (inter-platform competition) and to enable retail or resale competition over the regulated incumbent network (intra-platform competition). This proved very difficult to operationalise in practice, leading the Commission to revise its position and place greater emphasis upon inter-platform competition (see https://cerre.eu/wp-content/uploads/2020/06/170220_CERRE_BroadbandReport_Final.pdf). In telecommunications, the development of inter-platform competition was expected to take many years given the time required to construct networks, with inter-platform competition viewed as a means of promoting competition in the meantime. We note that these timing differences may not apply in the same way in digital markets.
[72] If we refer to the telecommunications example again, this dynamic strategy was pursued by the regulators under the so-called ladder of investment: Martin Cave, Encouraging infrastructure competition via the ladder of investment, Telecommunications Policy, 2006.
[73] We recognise that measures to promote intra-platform competition may also have other effects (such as to weaken incentives for the gatekeeper to invest in the Core Platform Service because they will be obliged to share rents with downstream competitors). These concerns would apply irrespective of whether or not there are other measures to promote inter-platform competition and so are not relevant to our concerns about the coherence of the different obligations.

Another well publicised example of a **trade-off arises with Article 6(5) DMA, which prohibits self-preferencing by search engine gatekeepers**. One interviewee explained to us that traffic generated by user searches can only be directed to a single recipient. This can either be a direct supplier such as hotel or airline or a third-party aggregator or vertical search provider. The overall impact of Google's efforts to comply with the obligation[74] has been that traffic to hotels or airlines has fallen (Google reports by up to 30%[75]) and that traffic to third-party aggregators or vertical search services has increased.[76] We make no comment on the merits of this situation beyond noting that measures to promote intra-platform competition between the gatekeeper and third-party vertical search sites do so potentially at the expense of direct suppliers who may find unable to avoid being charged a commission by the third-party vertical site to transact with the end user (whereas they had previously transacted directly without any such charges being payable.)[77]

This is a case where **the tension is not so much between different models of competition as between the interests of different groups of business users** (i.e. vertical search providers on the one hand and direct suppliers on the other). The Commission could consider - or the gatekeeper could request - producing a specification decision to clarify what the objectives of the measures are and how they may be expected to impact different groups of business users.

We do not criticise the Commission for failing to anticipate the inconsistencies or tensions that may arise when a particular gatekeeper applies a particular set of obligations to a particular core platform service. The obligations in the DMA are wide-ranging and take an indiscriminate approach to compliance, i.e. they do not attempt to discriminate between different gatekeepers and the same obligation may apply to many different core platform services. The interactions and the business models in digital markets are complex, and the impact of measures which are intended to change them is likely to only become apparent after the gatekeeper has taken steps to comply. However, there is a **risk that the impact of the DMA and the achievement of its objectives will be diminished if these inconsistencies and tensions are not explicitly recognised by the Commission, and if they remain unaddressed for too long once they become apparent**.

4.3. Taking Experience from Other Jurisdictions into Account

The implementation of the DMA in the EU is happening alongside the implementation of antitrust and regulatory measures in other jurisdictions such as the US, UK, Japan or Brazil.[78] The impact of those measures may inform the Commission's thinking about how to regulate in future. This may contribute to consistency of regulatory approaches across jurisdictions which may be beneficial for both the regulators and the regulated firms and, ultimately, their business and end users. Influence is

[74] P.171 at https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-bb_2024-3-7_2025-3-6_en_v1.pdf.
[75] https://blog.google/around-the-globe/google-europe/new-competition-rules-come-with-trade-offs/#:~:text=Hotels%20are%20concerned,expressed%20similar%20concerns.
[76] In an interesting new study, Joan Calzada, Néstor Duch-Brown2, Xavier Fageda, Nicandro Quirós, Who benefits from Google's SERP? The impact of the DMA on the Air Travel Market Markets, 2026 show that
the DMA prohibition of self-preferencing has generated strong redistributive effects, reallocating user attention towards smaller market participants of airline and flight comparison website.
[77] At paragraph 53 of its compliance report Google says 'Through the different changes outlined above, Google seeks to achieve a balance between the interests of end users and different business users, including VSSs and direct suppliers, that is fair, reasonable, and non-discriminatory. All the changes Google is making taken together – subtractions and additions – are what strikes this balance.': Para 53 p.180.
[78] https://www.oecd.org/en/topics/sub-issues/competition-and-digital-economy.html; Gunn Jiravuttipong, The Global Race to Rein in Big Tech, U. PA. J. INT'L L _ (forthcoming 2026).

flowing in both directions**.** For example, in the US the judge in the *Google Search* case explicitly referred to evidence about the lack of impact of search choice screens that are required under the DMA (and previous Commission competition cases) when rejecting them in that case.[79]

On the other hand, in the *Epic vs Google* case[80] the judge went further than the DMA in requiring so-called 'catalogue-access' to allow a user to download the app they are seeking in the third-party app store from the Google Play Store if the app is not in the third-party app store, thereby allowing users to have access to the same inventory of apps via both stores. This seems to stimulate inter-platform competition in app stores in ways that are potentially more effective than the combined DMA obligations discussed above. The order also prevents Google from paying app developers to favour the PlayStore over rival stores, which is not an obligation contained in the DMA. In November 2025, Google and Epic announced that they had reached a settlement on remedies which Google will apply globally, including in the EU. **In these circumstances it may become more difficult to discern the impact of the DMA, given that Google's conduct and the opportunities for competition will be influenced by legal commitments which arise from other legal sources** (recognising that in other cases the gatekeeper may not apply the same remedies globally). Any assessment of costs will also be more complex since Google will now be incurring costs to comply with US court orders in Europe even if its DMA obligations were to be withdrawn or modified.

Although there is likely to be some overlap and duplication of measures arising from actions which gatekeepers take in response to court orders or settlements in the US or elsewhere, the **different approach of the DMA means that there will still be many points of divergence**. The DMA requires all designated gatekeepers to comply with all relevant obligations for each core platform service, whereas US court proceedings focus on the actions of an individual firm and the measures required to remedy the anti-competitive effects of those actions. Thus, for example, Google has adopted measures for its app store which extend beyond those applicable under the DMA whilst Apple was subject to separate court proceedings in the same jurisdiction (the US) which have resulted in an order to implement much more limited changes.[81] It is not clear whether this arises from different views on the application of the law or from differences in business models or end user preferences of the kind which we discussed earlier in this paper.

[79] 'Choice screens are not likely to change the competitive landscape under current or even near-term market conditions. Plaintiffs' economic experts have acknowledged as much. Liab. Tr. at 6091:3-21 (Whinston) (testifying that choice screens would shift "less than 1 percent of the U.S. market share"); Rem. Tr. at 2187:4-17 (Chipty) ("We know from Europe that when users are given a choice today, they will overwhelmingly choose Google."). And the real world offers proof. The European Commission has mandated the display of choice screens on Android 191 devices since 2020,28 yet there has been little shift in market share away from Google', p.190-1 at https://www.texasattorneygeneral.gov/sites/default/files/images/press/Google%20Search%20Engine%20Monopoly%20Ruling.pdf.

[80] https://storage.courtlistener.com/recap/gov.uscourts.cand.364325/gov.uscourts.cand.364325.701.0_1.pdf.

[81] https://regmedia.co.uk/2021/09/10/epic-v-apple.pdf.

5. Conclusion

This issue paper highlights that a proper assessment of the DMA's impact, both positive and negative, is inhibited by limited publicly available evidence and the lack of a robust evaluation framework as well as the Commission's understandable focus on improving compliance, and an enforcement process that is (and will remain) iterative in nature. Gatekeeper compliance reports, while describing implementation steps, offer little quantitative insight into how end users and business users are responding to the changes mandated by the DMA, at least in their published versions. Without the Commission requiring the systematic and regular production of output indicators, such as CERRE has proposed in earlier papers, the debate on DMA impact risks remaining anecdotal and speculative. In principle, the Commission is in a position to provide a balanced and authoritative assessment of the impact of the DMA, as Article 53 DMA requires. But, so far as we know, it has yet to commit itself to doing so or begun the work that would be required to develop a robust, dynamic evaluation framework, supported by data to populate it.

As the paper emphasises, assessing impact also requires avoiding simplistic generalisations and recognising the heterogeneity of digital services, differentiated user preferences and the timing of behavioural responses, all of which make the assessment of the impact of the DMA a challenging exercise. Many obligations seek simultaneously to promote inter-platform and intra-platform competition, and their effects can interact in ways that can amplify benefits or introduce tensions. These complexities underscore the need for the Commission to begin efforts to introduce greater coherence across obligations and to address contradictions when they emerge, through either specification decisions or more targeted adjustments to the obligations themselves.

Looking ahead, the DMA's impact can be maximised through clearer legal interpretation, greater predictability for gatekeepers and business users and, over time, a more explicit use of proportionality assessments to target the law where it yields the greatest benefits. The current DMA review, due to be completed by May 2026, offers an opportunity to begin this work. By anchoring its assessment in quantitative evidence and an analytical framework which it has developed in consultation with interested parties, by clarifying expectations, and by ensuring coherence across obligations, the Commission can help ensure that the DMA matures into a more targeted, more impactful and more sustainable regulatory framework—one that fosters innovation, protects users, and supports a healthier competitive environment in Europe's digital markets.

Horizontal Interoperability of Social Networking Services

Marc Bourreau
Jan Krämer

1. Introduction

Among the obligations in the Digital Markets Act (DMA), **Article 7** stands out for its ambition and complexity, which shows as it is the only obligation laid out in a separate Article of the DMA. It mandates that gatekeepers offering **Number-Independent Interpersonal Communications Services (NI-ICS)**, such as messaging services, must ensure interoperability with rival services upon request and free of charge. To date only two services by Meta – Messenger and WhatsApp – are designated under Article 7.

The motivation behind Article 7 is to address the entry barriers constituted by network effects (aka **demand-side scale economies)** that incumbents enjoy due to large installed user bases. In digital communications, network effects can create significant barriers to entry: users are more likely to join platforms where their contacts already reside, reinforcing the dominance of established players. By mandating horizontal interoperability, Article 7 seeks to **level the playing field**, allowing users of smaller or newer services to communicate seamlessly with users on dominant platforms. This, in theory, should reduce switching costs, enhance user choice, and stimulate competition based on service quality rather than network size. This provision is inspired by the principle of **interconnection** in telecommunications regulation, where dominant network operators were required to allow competitors to connect to their networks to facilitate universal communication.

At the time of writing, roughly two years after Meta was first required to comply with Article 7 in March 2024, this provision has so far only shown limited market impact. Only two third-party messaging service providers, BirdyChat and Haiket, have started to implement horizontal interoperability with Meta.[82] However, interoperability through these services is not yet operational, and BEREC (the Body of European Regulators for Electronic Communications) continues to raise concerns regarding some aspects of Meta's reference offers (i.e., the terms and conditions, and technical implementation details of interoperability).[83]

Yet, in its scheduled DMA review, the Commission now considers whether it should extend the scope of Art. 7 to Social Networking Services (SNS).[84] This is due to the legislative history of Art. 7. The Commission's initial proposal of the DMA did not include horizontal interoperability obligations for messaging services. During the legislative process, a key proposal of the Parliament was to amend the DMA to include horizontal interoperability for NI-ICS as well as SNS. Then, in the trilogue, a political agreement was reached whereby only horizontal interoperability of NI-ICS was to be included in the DMA (now Article 7), and horizontal interoperability of SNS was to be reconsidered in the "near future".[85] In particular, Art. 53 of the DMA required the Commission to "evaluate if the scope of Article 7 may be extended to online social networking services."

In this issue paper, we examine the proposal to extend Art. 7 DMA to SNS in more detail, against the backdrop of experiences with implementing NI-ICS interoperability, as well as the extant academic literature. In doing so, we draw on our previous reports on NI-ICS interoperability (Bourreau, Krämer

[82] See https://about.fb.com/news/2025/11/messaging-interoperability-whatsapp-enables-third-party-chats-for-users-in-europe/
[83] See [83] https://www.berec.europa.eu/en/all-documents/berec/opinions/berec-opinion-on-metas-reference-offers-to-facilitate-messenger-and-whatsapp-interoperability-under-article-7-of-the-digital-markets-act
[84] https://digital-markets-act.ec.europa.eu/consultation-first-review-digital-markets-act_en
[85] https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users

& Buiten, 2022; Bourreau & Krämer 2023) in which we already highlighted the benefits and risks of horizontal interoperability of digital services more generally.

The remainder of this note is organised as follows: In Section 2 we briefly review the state of implementation of Art. 7 with respect to NI-ICS, as this is informative with regard to the experiences and challenges that can also be expected when extending Art. 7 to SNS. In Section 3, we highlight the key findings of extant literature on the benefits and risks of horizontal interoperability for digital services and how these map to the recent experience of implementing Art. 7. Finally, against this backdrop, we comment specifically on extending the scope of Art. 7 to SNS.

2. State of implementation of Art. 7

As noted above, the only number-independent interpersonal communication services (NI-ICS) that are currently designated as a core platform service are WhatsApp and (Facebook) Messenger, both offered by Meta. These services meet the thresholds laid out in Article 3 DMA, specifically exceeding 45 million monthly active end users and 10,000 yearly active business users in the EU. In the legislative process, it was widely believed that iMessage by Apple would also be designated, but after a thorough investigation the Commission accepted Apple's arguments that iMessage was indeed not an "important gateway" for business users to reach end-users. Meta has been required to comply with the interoperability obligation since 7 March 2024 for WhatsApp and since 6 September 2024 for Meta Messenger. With respect to Messenger, the Commission granted extension due to technical and security complexities.[86]

Since then, Meta provided several versions of its reference offers,[87] due to ongoing feedback and negotiations with the Commission and potential access seekers. BEREC has commented on various versions of the reference offers, as foreseen by Recital 64 of the DMA, with its latest opinion published in March 2025.[88] In this opinion, it noted improvements in regard to previous reference offers (such as implementation of typing indicators, read receipts or reaction messages in relation to Facebook Messenger, but not WhatsApp), but also notes that important (basic) features, such as editing or deleting messages, multi-device support for more than four devices, and discoverability of other users are still lacking from the reference offers, undermining the value of interoperability offers for both users and competitors.

Indeed, no major third-party NI-ICS has so far implemented interoperability with any of Meta's designated NI-ICS. Only two small, new players, BirdyChat and Haiket, have announced to be interoperable with Meta.[89] However, interoperability is not yet operational, as users of Meta's messaging services are still unable to opt-in to connect with users of third-party services through interoperability.[90]

BEREC recently expressed the view that the delay in the effective implementation of the interoperability obligation is partly due to poor technical implementation by Meta, but also because the scope of the interoperability provisions outlined in Article 7 is too limited.[91]

However, in our view, it is questionable whether the currently limited experience and impact of the horizontal interoperability provision in Article 7 of the DMA should be used as justification for extending its scope, whether it is by including additional features of NI-ICS or by expanding the provision to cover SNS. As we detail next, the challenges and pitfalls of implementing horizontal interoperability that come to the forefront now, have already largely been anticipated in previous reports and academic literature.

[86] https://ec.europa.eu/competition/digital_markets_act/cases/202426/DMA_100097_133.pdf
[87] https://developers.facebook.com/m/messaging-interoperability/
[88] https://www.berec.europa.eu/en/all-documents/berec/opinions/berec-opinion-on-metas-reference-offers-to-facilitate-messenger-and-whatsapp-interoperability-under-article-7-of-the-digital-markets-act
[89] As of December 2025, BirdyChat and Haiket had not officially launched; they had only opened a waiting list for interested users.
[90] https://about.fb.com/news/2025/11/messaging-interoperability-whatsapp-enables-third-party-chats-for-users-in-europe/
[91] https://www.berec.europa.eu/en/all-documents/berec/opinions/berec-response-to-the-european-commissions-consultation-on-the-first-review-of-the-digital-markets-act

3. Benefits and risks of horizontal interoperability of digital services

Horizontal interoperability (aka interconnection) regulation is a well-known remedy from telecommunications markets and has generally worked well in this context to allow for **competition in the market** despite the presence of strong network effects. This positive experience has inspired the co-legislators to also impose horizontal interoperability requirements for NI-ICS in the DMA, as NI-ICS are seemingly similar to traditional telecommunications services.

The pro-competitive effects of horizontal interoperability have been highlighted by academic literature and scholars (e.g., Graef 2015, Gans 2018, Crémer et al. 2000, Jullien and Sand-Zantman 2021, Scott-Morton et al. 2021). We summarise these in Bourreau, Krämer & Buiten (2022, Section 3.1.1). Generally, horizontal interoperability is believed to aggregate firm-specific network effects into industry-wide network effects, such that firms can compete in dimensions other than network effects. This also lowers entry barriers constituted by firm-specific network effects and lowers consumers' opportunity costs of switching providers. This should clearly benefit the contestability of the NI-ICS market.

However, the pro-competitive effects of horizontal interoperability also rest on assumptions, which may not be met to the extent assumed, and which may give rise to new (anti-competitive) trade-offs. Moreover, there are likely significant costs and complexities to implement horizontal interoperability of NI-ICS, due to technical challenges and regulatory oversight. We summarise the risks and challenges of horizontal interoperability in Bourreau, Krämer & Buiten (2022, Section 3.1.2), and detail the numerous technical challenges and trade-offs involved in Bourreau and Krämer (2023).

More specifically, in our view, two key features of digital services, such as NI-ICS and social networking services, set them apart from other services, especially telecommunications services, where horizontal interoperability regulation has been successfully applied in the past, and require a re-evaluation of the benefits and risks of mandating horizontal interoperability.

First, **digital services are generally much more complex**, i.e., they have **a higher feature-richness**, than telecommunications services. Second, digital services often **allow for easy and low-cost multihoming** (i.e., using different services in parallel on the same device), which presents an alternative to interoperability. We elaborate on why each difference matters in more detail below.

3.1 Digital services are more complex than telecommunications services and allow only for imperfect interoperability

Even when services appear to meet similar user needs, they differ in functionalities and features (e.g., encryption standards, message formats, emoticons). Interoperability can only ever cover a common set of core features, and each feature innovation by a firm risks requiring renegotiation of the interoperable set of features. Unlike standardised telecommunications services, digital services can therefore at best achieve imperfect interoperability.

This is implicitly already recognised by the DMA, as it requires gatekeepers only to make "basic functions" interoperable, and even this shall only occur in three phases, whereby first only end-to-end text messaging between individual users is subjected to interoperability requirements, and group messaging and video calls being included 2 years and 4 years later, respectively. The current experience from the implementation of the first phase of Art. 7 shows that even for "basic" text communication and roughly two years after the compliance deadline, interoperability of NI-ICS is still patchy, and important "basic" features, such as the deletion or editing of messages, are not interoperable. Also, the lack of discoverability of contacts on other networks, as it the case in the current reference offer, limits the effectiveness of interoperability and has already been anticipated in Bourreau & Krämer (2023).

Imperfect interoperability is not only a result of the limitation of the scope to "basic features", but also due to a lack of incentives of the regulated gatekeeper to offer the best interoperability experience possible (known as incentives to "sabotage" in the academic literature), and due to the actual technical complexities involved. While some scholars have pointed to the fact that readily available interoperable communication protocols exist (e.g., the MATRIX protocol), this misses the point that in the present context, gatekeepers must open up their existing systems, which have not been designed with interoperability in mind. Here, no readily available solutions existed prior to the DMA (cp. Bourreau & Krämer 2023). In a similar vein, one could argue that messaging functionalities could, in principle, be standardised, which would facilitate interoperability. However, the services that need to be made interoperable today are not standardised, making this path, at best, a long-term objective.

Albeit interoperability of basic text communication is still unsatisfactory one year and a half after the compliance deadline, in one year and a half group chats are supposed to become interoperable, for which there are numerous additional complexities in the implementation (cp. Bourreau & Krämer, 2023, Section 3). It is foreseeable that interoperability will become even less functional in this case. Generally, the degree and usefulness of interoperability is likely to become the lower, the more complex and feature-rich the services are.

In addition, for digital services, innovation is rapid, and numerous new features have been added into WhatsApp and Messenger, as well as other messaging apps, since political agreement on the DMA was reached. Some (but not all) of these features may also be significant for the experience when communicating with users on other networks (such as being able to retract or edit a message). The way in which newly integrated AI features will change how we use messaging apps and how this affects interoperability is yet to be determined. Currently, integrated AI seems more to play the role of a chat function, which does not decisively impact communication off-net. However, this may change with future implementations. In any case, defining the set of interoperable features will remain cat-and-mouse game, on which regulators will always lag behind.

The inherent imperfectness of interoperability for digital services (contrary to standardised telecommunications services) has several important implications for the applicability and effectiveness of mandated horizontal interoperability in practice. Most importantly, **if interoperability remains imperfect, installed-base advantages persist.** Users may still favour the dominant provider to access the full set of functionalities, even if entrants offer superior quality or features, since these advantages apply only to a limited user base. Interactions with the incumbent's larger base remain

constrained and thus undermine the effectiveness of interoperability regulation for fostering contestability and competition in practice.

Further, due to the technical complexities involved, rapid addition of features and functionalities for digital services, and gatekeepers' lack of incentives to provide the best degree of interoperability feasible at any point in time, interoperability is not only likely to provide a persistently poor user experience, it also comes with **significant costs of implementation and enforcement,** as the proportionate and effective degree of interoperability will have to be constantly reviewed (by the Commission and entities such as BEREC) and re-negotiated with the gatekeeper. Even when services are standardised, experience from telecoms regulation shows that incumbents regularly engage in subtle "sabotage" of interoperability. In addition to not implementing features that are relevant for the user experience pointed to above, there are also other, more subtle ways in which the gatekeeper may interfere with interoperability, ranging from small technical „difficulties" that break interoperability every so often, to dark patterns (e.g., in collecting consumer consent or making it cumbersome for consumers to detect others on rival networks). Enforcement is therefore resource-intensive and costly—justifiable only if benefits are substantial, which, as argued above, remains doubtful.

Finally, the technical complexities and trade-offs involved also bear additional risks for consumers, as interoperability comes with **unavoidable compromises in security and privacy** (cp. Bourreau & Krämer 2023). Article 7(3), which requires that security levels "shall not be reduced," is unrealistic in practice. Interoperability expands attack vectors and thus reduces overall security. While specific protections, such as end-to-end encryption, may be preserved in principle, this depends on robust key management and trusted endpoints, which become increasingly difficult with more actors involved. This is one of the main reasons why privacy-focused messenger apps like Signal and Threema have announced, even before the DMA came into force, that they would not seek interoperability with NI-ICS services of gatekeepers.

Interoperability also comes with unavoidable compromises in privacy, as user data and meta data is handled by more entities. For example, WhatsApp collects third-party registration information such as username, messages and media within messages, connection data such as blocked users and groups created, device information such as IP-address and location.[92] User consent to such data sharing is mandatory for interoperability to work.

3.2 For many digital services, multihoming presents a viable alternative to interoperability

Unlike telecom services, users of digital services often "multihome," i.e., use multiple digital services concurrently, because doing so requires little effort or cost. For example, a representative survey by the German Federal Network Agency (2021) shows that 73% of users of messaging services multihome, interacting across different networks without the need for interoperability. Multihoming

[92] https://www.whatsapp.com/legal/dma-notice-non-users?lang=en

is further facilitated by business models where services are typically offered free of charge, with monetisation instead based on advertising or data collection.

Relative to interoperability, multihoming requires users to maintain multiple accounts and manage different updates. However, it also presents several advantages over interoperability, both for users and for third-party providers that are intended to benefit from interoperability regulation.

First, unlike interoperability, **multihoming allows users to access the full feature set of each service**, including the new features when they become available. Innovation and competition can therefore unfold more freely and is not mediated through interoperability. Gatekeepers have no control over the user experience at the rival service, as they would have in the case where they control the interface through which interoperability is realised. Issues of sabotage and poor implementation do not arise. Thus, through multihoming digital services can compete directly for consumers on the basis of quality, which also explains why several alternative messaging apps, such as Signal, Threema and Telegram, have successfully managed to attract a significant user base – despite the presence of network effects.

Unfortunately, as demonstrated in Bourreau and Krämer (2025), **interoperability can have a negative impact on market contestability driven by multihoming. This is because interoperability is likely to reduce users' incentives to multihome.** Some consumers (with low valuation for enhanced features) that would have multihomed in the absence of interoperability, may now choose to singlehome on the incumbent network if they can still reach contacts through multihoming (albeit with a limited set of features). This reduces the overall number of users on the rival network, and through network effects, also the value of the network for all other users that remain on the rival network. Through this negative feedback loop, mandatory interoperability can backfire by reducing contestability rather than enhancing it for services that already have a sizeable user base. This presents a second, more strategic reason, why the most promising rival firms providing messaging apps, are not interested in requesting interoperability under Art. 7 DMA, and which has been explicitly voiced by Threema CEO Martin Blatter already in 2022.

A second, important reason why multihoming has benefits over interoperability is that users prefer to keep different digital (communications) services separate, as they are using them for different purposes and to interact with a different group of people. Many users therefore do not see much value in interoperability or are even against it (Tas et al 2024). This offers a third explanation, why third-party NI-ICS providers may be reluctant to undergo the efforts of requesting and implementing interoperability. Although users can always opt-out of interoperability (as demanded by Art. 7), implementing interoperability only is worthwhile if it is actually demanded by the vast majority of users.

4. Extension of Art. 7 to Social Networking Services SNS

Against this backdrop, we now consider a possible extension of Art. 7 to SNS more specifically. The analogy of SNS to NI-ICS is evident. SNS are also a type of "communications service" that is characterised by strong network effects and large installed bases of the incumbent services, in particular those already designated as SNS core platform services under the DMA: Facebook, Instagram, TikTok and LinkedIn.

Accordingly, SNS are also subject to market tipping effects, and network effects can present entry barriers, driving the notion that interoperability may help in rendering these markets more competitive. However, the already highlighted risks and challenges associated with interoperability also apply in the context of SNS and are likely to be exacerbated compared to NI-ICS. This is due to a number of reasons.

First, SNS are much more complex and feature-richer services than NI-ICS, such that interoperability is even more fragmented and it is even more difficult to implement and maintain interoperability than for NI-ICS. For example, while NI-ICS are relatively homogenous in the way that they present content (message by message in chronological order), the display of content varies greatly between the designated SNS. While in Facebook and LinkedIn the content format is mixed (text, image and video), Instagram pursues a "visual-first" approach (image and video), while TikTok's content is "video-only". Despite some similarities (e.g., content can be liked, commented on and shared on the network), the form in which this can be done also varies considerably, and is subject to rapid change and evolution.

Second, unlike NI-ICS, which typically show every message sent by a user to all users for which the message was intended, and in chronological order, **SNS employ content curation** (i.e., not every post sent is seen by all users following that user in the social graph) and **personalised recommendations** (i.e., even content by users not in the user's social graph may be seen). **This complicates the very notion of interoperability even further**, and those features of SNS would provide designated gatekeepers with even more sophisticated and subtle ways to „sabotage" interoperability, e.g., by shadow banning content from interoperable networks.

Third, different SNS tend to be even more heterogeneous in which user groups they appeal to than NI-ICS. Empirical evidence suggests that **users value the distinctiveness of SNS**, using different platforms to connect with different groups and for different purposes (see, e.g., Kroon & Arnold, 2018). TikTok's user base tends to be very young, compared to that of Facebook, with Instagram being in the middle. LinkedIn caters to job seekers and professionals, while the others are more catering to private users. This segmentation of the market and differentiation of services is not surprising in the presence of strong network effects, as otherwise users would have gravitated to only one SNS if they were similar. This also means that basic interoperability with a minimum, common subset of features is likely to be even less valuable in the context of SNS than it is in the context of NI-ICS, and what features are important are likely to be valued differently by the different heterogeneous user groups.

Defining and negotiating the set of features that are subject to interoperability across different (and deliberately differentiated) existing core platform SNS is therefore likely elusive in the context of SNS and would in any event need to be done on a case-by-case basis.

One might argue that instead interoperability should be defined on a SNS-by-SNS basis in order to stimulate competition and contestability *within* a SNS-type that caters to a similar user group. While this seems more practical (but yet more complex than in the case of NI-ICS), it is also important to note that to begin with, the set of potential rival SNS to one of the gatekeepers' seems much smaller and less developed than in the case of NI-ICS, where sizeable competitors already exist, like Signal and Threema. Hence, in this case, interoperability regulation would firmly bet on the hope that interoperability would stimulate entirely new entry of SNS that are similar to those to which they seek interoperability with. But such entry seems very unlikely, as it is highly risky to enter with a little differentiated service that would strongly depend on patchy and fragile regulated interoperability. Also here, we deem it more likely that **competition for the market** takes place (via multihoming, rather than interoperability), with a service that is sufficiently different to an existing core platform SNS – as was in recent history the case with TikTok, who pioneered the "video-first" approach, catering specifically to a young user audience.

The experience of telecommunications access regulation offers valuable insights here. Access regulation has proven most effective in developing competition when access seekers were both able and incentivised to differentiate themselves by investing in their own network infrastructure (facility-based competition). In contrast, service-based competition, where access seekers have limited opportunities for differentiation, has generally been less successful.

In addition, given the experience from NI-ICS, where the Commission only had to deal with one gatekeeper, offering two NI-ICS, each with a lower complexity and feature-richness than that of any of the designated SNS, does not make it likely that a meaningful reference offer can be developed in a reasonable amount of time. In summary, **the technical challenges, implementation costs, and enforcement burdens would be even greater for SNS than for NI-ICS.**

Finally, interoperability of SNS may also present new risks for users, above and beyond the security and privacy risks already mentioned in the context of NI-ICS. A further concern is that **SNS interoperability could aggravate known societal harms on SNS such as disinformation, hate speech, privacy risks, and addictive usage patterns**. By blurring accountability for content moderation, and requiring to host content that originated on another platform, interoperability could reduce each platform's responsibility for the content it hosts. At the same time, SNS have stronger incentives to prevent leakage of content and consumers from one SNS to another, designing their systems even more addictive, so content and consumers stay „on net" rather than to consume content „off net".

Meta's announcement in March 2024 that Threads had "entered the fediverse" highlights the practical challenges of interoperability among social networking services. Interoperability with Mastodon is still one-sided: content from Mastodon does not appear on Threads, and only instances that have chosen not to defederate display Threads content. This situation also raises important concerns regarding content moderation. Mastodon instances, in particular, face a large influx of content from Threads that they must moderate according to their own policies, which could overwhelm the capacity of their volunteer moderators. While research on this type of issue is yet scant, these problems are likely to arise, with potentially important consequences. In any case, they render the potential benefits of SNS interoperability even more doubtful.

5. Conclusions and recommendations

Taken together, we believe the arguments presented offer the firm conclusion that the expected benefits of extending Art. 7 DMA to social networking services are rather low, while the expected costs and risks are substantial. The difficult experience from implementing and enforcing Art. 7 in relation to NI-ICS, which are compared to SNS less complex and share more common features among rival services, shows that these concerns are real and material. Roughly two years after the compliance deadline, only two small third-party NI-ICS provider have taken up interoperability, and still it is not yet operational. We do not think that this is due to a lack of scope of the interoperability mandate, but rather to structural issues and differences between telecommunications services (for which the experience with interoperability or interconnection regulation is overall positive) and digital services. Therefore, we do not recommend broadening the scope of Art. 7 to SNS.

6. References

Blankertz, A. & Windwehr, S. (2025, May). Interoperability and openness between different governance models: the dynamics of Mastodon/Threads and Wikipedia/Google. Social Science Research Network. https://ssrn.com/abstract=5238447

Bourreau, M., Krämer, J., & Buiten, M. (2022, March). Interoperability in digital markets (CERRE Report). Centre on Regulation in Europe (CERRE). https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf

Bourreau, M., & Krämer, J. (2023, December). Horizontal and vertical interoperability in the DMA (CERRE Issue Paper). Centre on Regulation in Europe (CERRE). https://cerre.eu/wp-content/uploads/2023/12/ISSUE-PAPER-CERRE-DEC23DMA-Horizontal-and-Vertical-Interoperability-Obligations.pdf

Bourreau, M., & Krämer, J. (2025, June 15). Interoperability in digital markets: Boon or bane for market contestability? (SSRN Scholarly Paper No. 4172255). Social Science Research Network. https://ssrn.com/abstract=4172255

Crémer J, Rey P, Tirole J (2000) Connectivity in the commercial internet. Journal of Industrial Economics 48(4):433–472.

Federal Network Agency (2021). Use of online communications services in Germany 2021 consumer survey results. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_kurz21-ENG.pdf?__blob=publicationFile&v=2.

Gans J (2018) Enhancing competition with data and identity portability. The Hamilton Project, Policy Proposal 2018-10, Brookings Institute.

Graef I (2015) Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. Telecommunications Policy 39(6):502–514.

Kroon, P., & Arnold, R. (2018). Die Bedeutung von Interoperabilität in der digitalen Welt – Neue Herausforderungen in der interpersonellen Kommunikation (WIK Diskussionsbeitrag Nr. 437). WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH. https://hdl.handle.net/10419/227048

Scott Morton FM, Crawford GS, Crémer J, Dinielli D, Fletcher A, Heidhues P, Schnitzer M, Seim K (2021). Equitable interoperability: the “super tool” of digital platform governance. Tobin Center for Economic Policy, Discussion Paper No. 4, http://dx.doi.org/10.2139/ssrn.3923602.

Tas, S., Wiewiorra, L., & Liebe, A. (2024, July 31). Interoperability for number-independent interpersonal communications services under the DMA: More harm than good? Proceedings of the TPRC2024: The Research Conference on Communications, Information and Internet Policy. Available at SSRN. https://ssrn.com/abstract=4911632

Open Tech Platforms: Technology and Governance Mechanisms

Zach Meyers

1. Introduction

EU policy makers want to see more intense competition in the digital sector – and to do so by making platforms more open. By "openness" this paper refers to the easing of restrictions on – or even the active facilitation of – the use of a platform's data or functions by third parties. "Openness" in this context can help users mix-and-match different products and services from different brands, and to more easily switch between competing devices and services. In the context of the growing geopolitical tensions between the EU and the US, making large tech platforms more open may offer a way to give digital ecosystems more resilience, by avoiding users being stuck in the services of a single ecosystem; if users are diffused across multiple competing services then the consequences of disruptions can be less severe. From the perspective of EU competitiveness, openness could give European tech firms greater opportunities to enter and compete in a sector with very high productivity. And from a consumer perspective, there is evidence that users value the ability for their tech products to work well with other products, regardless of their brand.[93]

The Digital Markets Act pursues three ways to open up tech platforms:

- Rules on '**data portability**' can help end-users[94] and business users[95] extract data or move it from one service to another. This can help users to switch between competing services or use multiple competing services at the same time (known as 'multi-homing'), reducing 'lock in' effects. It can also generate innovation, by enabling users to send their data to service providers who can unlock new business models with it;[96]
- Rules on '**horizontal interoperability**'[97] aim to allow providers of online communications services like instant messaging[98] to choose to interoperate with a competing gatekeeper service. For example, the provider of a service like Telegram could choose to allow its users to communicate with users of WhatsApp; and
- '**Vertical interoperability**'[99] means that operating systems (like iOS, Android and Windows) must give service and hardware providers (which could include competitors to the gatekeeper who offer alternative services or devices to those of the gatekeeper at various points in the ecosystem) access to the same functionality that those providers give to their own apps and services. The goal of this provision is to ensure third-parties can build products and services which are competitive with those made by operating system gatekeepers.

This paper does not focus on the merits of mandating a greater degree of openness and the scope of the DMA's openness mandates. Mandating a greater degree of openness may sometimes – but will not always[100] – promote incentives to innovate and invest. Instead, this paper asks how such openness can be achieved in a way which is efficient, effective, and respects users 'privacy and security.

[93] CODE, 'Consumer perceptions on hardware interoperability - poll results', 14 February 2025, available from https://www.opendigitalecosystems.org/updates/13/consumer-perceptions-on-hardware-interoperability--poll-results.
[94] Art 6(9).
[95] Art 6(10).
[96] Jan Krämer, Pierre Senellart and Alexandre de Streel, 'Making data portability more effective for the digital economy', CERRE Report, 2020.
[97] Art 7.
[98] Known in the DMA as 'number-independent interpersonal communications services' or NIICS.
[99] The DMA also requires 'horizontal interoperability', in the case of certain communications services under DMA art 7, which is beyond the scope of this paper.
[100] Carmelo Cennamo and Zach Meyers, 'Mandating Openness in Regulated Markets', CERRE, forthcoming.

Portability and interoperability both require the transmission of data. This requires the provision of technological and commercial mechanisms to facilitate that transmission in a safe and effective way. These mechanisms need to solve problems such as identifying and authenticating the recipient of the data; providing interfaces for the transmission of information; and determining the format of the data so that the recipient can recognise it, understand it and (in the case of interoperability) use it to interact with an operating system's functionality. The DMA is largely silent on the specific mechanisms which gatekeepers must use to provide more openness.

Governance mechanisms are also essential for two reasons. The first is so that there is a process for making decisions about the right technical and commercial mechanisms for openness. Decisions about which commercial and technical mechanisms to use must weigh their respective benefits, opportunities, costs and risks – and may sometimes involve trade-offs between the interests of gatekeepers, business users and end users, and sometimes between different members of these groups. The second purpose for governance mechanisms is so that **disputes about how these mechanisms operate in practice can be resolved**. In both cases, the design of governance mechanisms needs to ensure that the range of stakeholders' interests is adequately reflected.

To date, the Commission has largely allowed gatekeepers to adopt their own bespoke approaches to DMA compliance. However, the Commission has been more interventionist with certain aspects of vertical interoperability: it issued two specifications as to how Apple must comply with the rules on vertical interoperability, and currently proposes to specify how Google must comply. Generally, while gatekeepers have had some (and in some cases more extensive) engagement with business users and the Commission, the governance process by which gatekeepers have designed their approaches to openness has largely been led by gatekeepers' proposals or by the Commission. These were the most plausible short-term approaches when the DMA came into force. However, to give business users more confidence in the opportunities the DMA is supposed to deliver them, the Commission should encourage a more open, inclusive and transparent way of making decisions about governance, in ways which can promote as much consensus as possible between gatekeepers and business users. There are promising initiatives like those pursued by the Data Transfer Initiative – which provides a single and relatively seamless way of porting data between different services, including those of various gatekeepers – which illustrate that a gatekeeper- or Commission-led approach is not the only feasible approach. The co-operation between Apple and Google to make switching between mobile ecosystems easier also illustrates that, at least in some cases, industry can make substantive progress through co-operation.

In making this shift, the Commission will need to have regard to certain risks. Institutionalised and consensus-based decision-making can give business users more confidence: but if designed poorly they can slow decision-making, limit the ability for gatekeepers to differentiate their services, and constrain opportunities for gatekeeper-led innovation. The extent of these risks will vary based on the maturity of the particular sector, the current speed of gatekeeper-innovation, and the degree of differentiation. This implies that a shift towards a more institutionalised, inclusive, and consensus-driven approach should not necessarily happen at the same pace – or have the same end point – for all types of gatekeeper services.

2. Openness Requirements Under the DMA

The DMA tries to ensure that gatekeeper's core platform services are more open. In this context, "open" means that the DMA requires the gatekeepers to relieve restrictions on – or even actively facilitate – the use of data provided by users, and the gatekeeper's own assets, by third parties. As this section shows, however, the DMA's rules have a number of conditions and qualifications which reflect that openness also involves risks and costs which need to be managed.

2.1 Portability and Switching

In the case of portability, openness means allowing an end user to extract data about their own use of a service, or "port" that data directly to another service (where the user directs the gatekeeper to send the user's personal data directly to the third-party service). The data must be:

- Requested by the user;
- Given to the user directly or to a third party authorised by the user;
- "Provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service"[101];
- Made available through "tools to facilitate the effective exercise of such data portability";
- Made available through the provision of "continuous and real-time access"; and
- Provided consistent with the General Data Protection Regulation (GDPR), which in some cases (such as where data may be transferred overseas to a jurisdiction with lower data protection requirements) may be in tension with the DMA.

Similar portability rights exist for data of business users.[102]

The GDPR already provides a right for users to port their data in a "structured, commonly used and machine-readable format".[103] However, among other differences, the DMA rules also require gatekeepers to provide "tools" to export their data, and to allow users to direct data to be ported directly to a third party service.[104] This is essential, particular for end users, since the amount of data in question can be significant and end users increasingly rely on devices like smartphones where downloading and re-uploading data between services can be unwieldy.

2.2 Horizontal Interoperability

A reason users might be unwilling to switch is that – in the case of platform services like instant messaging that bring users together – a user might be unwilling to switch to a service if they would lose the ability to communicate with contacts who are not already using the competing service. To address this problem, DMA art 7 requires the "basic functions" of certain gatekeeper communications services to be progressively made interoperable with competing services.[105] The purpose is so that a

[101] DMA art 6(9).
[102] DMA art 6(10).
[103] GDPR art 20; see https://cerre.eu/publications/effective-and-proportionate-implementation-of-the-dma-3/.
[104] Under the GDPR, service-to-service transfers only need to be provided where "technically feasible".
[105] CERRE 2023 report on horizontal interoperability.

user on a third-party messaging service can still communicate with their contacts on a gatekeeper's service. This requires that:

- There is clarity about the "basic functionalities" that must be made available (in particular which features of those "basic functionalities", such as delivery and read receipts; disappearing messages; and so forth);
- Security levels are not compromised, including end-to-end encryption;
- The gatekeeper produces a "reference offer", a standing contract setting out the terms and conditions on which interoperability is available; and
- End users remain free to decide whether to make use of interoperability.

2.3 Vertical Interoperability

A final example of openness is that the DMA allows users to 'mix and match' a gatekeeper's platform service with complementary services provided by third parties, such as third-party apps or accessories on a smartphone. A user's willingness to do so may be hampered if the third party cannot provide the same functionality as a first-party app or device, however.

The DMA therefore requires gatekeepers operating systems to provide vertical interoperability.[106] This means gatekeepers which provide operating systems must give app and accessory developers access to equally effective access to hardware and software features that those providers make available to their own apps and services. In doing so, third-party service and hardware providers should be able to build services and accessories which provide a competitive offering to end users.[107] These rules aim to ensure a more "level playing field" between a gatekeeper's apps and devices, and those of third parties.

This requires that:

- There is a reasonable level of clarity about which functionalities business users are entitled to request. While a definitive catalogue may be disproportionate to produce, a list of major functionalities available to third parties could avoid third parties having to try to work out for themselves which operating system functionalities are used to by the gatekeeper to produce certain functions or features for end users;
- There is a process for assessing requests and whether they fall within the DMA;
- Security is maintained, particularly since access to system resources and functionalities can have significant privacy and security implications; and

Software tools such as 'application programming interfaces' or APIs are developed to enable business users to make use of interoperability.

[106] DMA art 6(7).
[107] DMA recital 55.

3. Technical and Commercial Mechanisms

Each of the openness obligations set out above entails addressing a series of significant technical and commercial implementation questions, so that openness is both effective and safe. Many of these questions are common across the different types of openness obligation. The DMA, however, provides little detail on how each of these complexities should be resolved and addressed. The purpose of this paper is not to provide definitive views on how the right technical solutions – but rather to highlight the complexity of the questions which need to be resolved, as background for discussion about how well-designed governance mechanisms could help address these questions.

3.1 Which Data and Functionality?

An initial question is about the scope and type of data or functionality which needs to be accessible to the end user and/or third parties. For example, the data portability rules require gatekeepers to provide data "provided directly by the user" and data "generated by the end user through their activity on the core platform service". There is, however, no explanation of which data this includes or excludes. For example, the wording appears to deliberately exclude data derived from the end user's activities or inferred by the gatekeeper, but there is no clear exception to protect the gatekeeper's own business secrets or information which might be personal data of a third party (such as the other party in a conversation). Similarly, it is not clear whether third party data is included (which is relevant since a lot of ported data, such as conversation histories with others, may contain the data of multiple persons).

The recent consultation draft guidelines issued jointly by the European Data Protection Board (EDPB) and the European Commission on the interplay of the GDPR and the DMA (the **Draft Guidelines**)[108] say that "gatekeepers are legally obliged … to give access to personal data of individuals other than the end user upon a request of the end user or of an authorised third party, if there is personal data concerning those other individuals in the relevant dataset". The Draft Guidelines do require gatekeepers to provide tools so that third party personal data can be excluded, but do not mandate its exclusion. It is unclear if this position can be maintained in the final guidelines, given it may contradict many users expectations and implies a high degree of trust in the recipient service which may not always be warranted.

Similarly, it will not always be clear for vertical interoperability which features and functionalities a gatekeeper makes available to itself (and, if these features are not *actually used* by the gatekeeper, producing a definitive "catalogue" may be difficult).

In all cases, there is also a question about the format of data and information to be transmitted or exchanged. Both portability and interoperability require defining data formats so that (for portability) the recipient can understand the data received and make use of it, and (for interoperability) to enable interaction with the operating system or communications service. Gatekeepers' core platform services (even those with relatively similar functionality) have not typically been designed to conform to any particular data standards for portability or horizontal interoperability. Their internal dataflows do not

[108] European Commission and European Data Protection Board, 'Joint guidelines on the interplay between the Digital Markets Act and the General Data Protection Regulation', version for public consultation, 2025.

necessarily map onto those of competitors easily. As explained in an earlier CERRE issue paper, this can be addressed through:

- The gatekeeper providing data 'as is', with the recipient service left to work out how to decipher and use it;
- The gatekeeper working with and facilitating the use of intermediaries or 'data adapters'. An example of such a service is the Data Transfer Initiative (DTI), which provides a 'bridge' to allow direct porting of data between some Facebook and Google services, for example;[109]
- The gatekeeper adapting its data to the needs of recipient. This is generally not a viable solution, at least in the short term, given the number and diversity of recipient services.[110]

In relation to horizontal interoperability, gatekeepers will need to take steps to make available a protocol for managing cryptographic keys between gatekeepers and third parties so that end-to-end encryption is available, and many services already use one of the few widely used protocols. For vertical interoperability, operating systems – including those of the gatekeepers – typically have a wide degree of openness to third-party developers already (although in some case that openness may be conditional on restrictive contractual or technical requirements). This means that there are established interfaces – known as application programming interfaces or APIs, which are codified instructions that enable third parties to exchange information with functionality provided through an operating system, and which typically provide a degree of stability even if the underlying operating system changes. While these APIs already exist, some gatekeepers have needed to extend and enhance them in response to the DMA.

3.2 Designing an Interface and Process

Secondly, gatekeepers are required to produce an interface and tools with which an end user can request portability, or an authorised third party can request data or interoperability. Rules on data portability expressly require gatekeepers to create tools to facilitate the exercise of these rights, for example through web portals. However, requests may also come via third parties – for example, a user might be using a competing third party service, and the service could offer to 'import' their data from a gatekeeper's service.

The design of these tools and their user-friendliness can play an important part in ensuring users are willing to use them. As noted in the Draft Guidelines, "Gatekeepers should not engage in behaviours that would undermine the effectiveness of the DMA's obligations, including the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function or manner of operation of a user interface or a part thereof to subvert or impair user autonomy, decision-making, or choice".[111] This raises particular concerns in the context of protecting security and privacy, discussed below, since "non-neutral" is not a term which can be easily understood. Gatekeepers may have both legitimate grounds for ensuring end users are protected, but pretextual security warnings may be used to discourage portability and interoperability. It is essential,

[109] https://dtinit.org/.
[110] Zach Meyers, 'Which Governance Mechanisms for Open Tech Platforms?', CERRE, January 2025.
[111] Draft Guidelines, para 125.

in that context, that any friction imposed on end users (who have already chosen to port or make use of interoperability) is proportionate to the risk.

From a technical perspective, tools like software development kits (SDKs) and application programming interfaces (APIs) are in practice necessary to facilitate portability and interoperability with third parties. Theoretically**, options include:**[112]

- The use of protocols mutually agreed between the gatekeeper and third parties. However, this approach does not seem viable for many large digital platforms today in practice, given that many of them offer unique sets of functionalities and were not initially designed with a view to ensuring data portability or interoperability across different platforms, and given the diversity of users which might take advantage of portability and interoperability. Some elements of functionality on devices – such as WiFi and Bluetooth – rely on widely adopted industry standards, but even then, the APIs used to access them across different operating systems vary significantly.
- Access seekers designing their own APIs, which gatekeepers would have to redesign functionalities within their platforms to accommodate. This solution is probably only viable where there is a relatively small number of legitimate potential access seekers which could design high-quality and secure APIs, or widespread agreement between access seekers about APIs that would work with particular services, and therefore it is not currently a suitable approach for many markets today where the number of access seekers is very large.
- Gatekeepers designing and providing their own interfaces and tools such as APIs to facilitate portability and interoperability. In practice, this is likely to be the most plausible way for gatekeepers to deliver portability and interoperability today since gatekeepers tend to have the most resources available to build high-quality and secure APIs and the best understanding of their own platforms. However, this could be combined with the use of 'bridges' or common approaches in some areas such as security vetting or portability across services: both ideas being pursued by the Data Transfer Initiative.

Gatekeeper-led APIs are likely the most practical and optimal way for gatekeepers to comply with the DMA in the short term – though this means that third parties bear the costs of making their services compatible with a variety of APIs/technical solutions. As described below, moving towards standards and mutually agreed industry-wide protocols in the long run would therefore prove more beneficial in some cases. In the meantime, end users and business users need comprehensive documentation on how to use the gatekeeper's tools – such as transparent access conditions, timeframes, technical requirements and limitations, and information on the outputs available.

3.3 Authentication and Security Screening

Gatekeepers must also have a process to ensure that the transfer of data and access to functionality is safe. At a minimum, such a process is needed to ensure gatekeepers can ensure compliance with both the GDPR and the DMA at the same time – but there are also questions about whether

[112] Ian Brown, 'The Technical Components of Interoperability as a Tool for Competition Regulation', OpenForum Academy, November 2020, see also https://www.berec.europa.eu/system/files/2023-06/BoR%20%2823%29%2092%20BEREC%20Report%20on%20interoperability%20of%20NI-ICS.pdf.

gatekeepers should be able to impose security requirements to protect end users and/or avoid reputational risk (as contemplated in DMA article 6(7) for example).

In the case of data portability, there are three steps to consider:

- The first is **authentication**, which may be essential so that the gatekeepers can be certain that a user has authorised the release of their own data – without consent, porting data would not only be unnecessary under the DMA but also, in most cases, unlawful under the GDPR. Particularly where the request comes directly from a third party, this could justify a gatekeeper seeking to understand and verify the third party's process for obtaining consent, and seeking to ensure the third party is who they say they are.
- A second question is whether the gatekeeper should be concerned about the **standard of data protection** observed by the recipient of the data and their level of trustworthiness. For example, can gatekeepers preclude or provide warnings if a portability request would result in data being moved to a jurisdiction with lower data protection standards? As an extreme example, the question arises whether a gatekeeper is obliged to facilitate a transfer to a third party which is known to act unlawfully.
- A third question is whether gatekeepers should be concerned about whether the third-party recipient of ported data is **genuinely providing the service they are advertising** to the consumer and the consumer fully understands what uses of their data they are consenting to.[113]

In the Draft Guidelines, there is a recognition that gatekeepers have a legitimate need to onboard third party recipients of data[114] and ensure "authentication procedures (including to verify the authorisation granted by end users to a requesting third party)".[115] This reflects that gatekeepers may often have stronger incentives than some business users to protect the overall security of a platform.

The draft also says that a gatekeeper "has to ensure appropriate information about the recipients of the ported data".[116] However, the Draft Guidelines imply this is largely meant only to ensure transparency to users. The Draft Guidelines state that gatekeepers are "not responsible for compliance of the authorised third party or the end user with data protection legislation" and expressly states that gatekeepers:

> "Should … not gather information pertaining to the authorised third party's compliance measures under the GDPR, including potential administrative or judicial proceedings the third party has undergone in relation to compliance with the GDPR, or whether the third party has suffered breaches of data security in the past".[117]

This is surprising given that credible bodies like the Data Transfer Initiative have developed models for industry-wide portability which recognise that the trustworthiness of a data recipient is a relevant consideration, and cross-industry bodies like the Coalition for Online Data Empowerment (CODE) have developed an 'Ethical Data Badge' initiative to allow firms to be accredited as trustworthy. Furthermore, the DMA's interoperability rules – which have similar potential for privacy and security

[113] Data Transfer Initiative, 'A third-party trust model for direct personal data transfers'.
[114] Para 130.
[115] Para 132.
[116] Para 113.
[117] Draft Guidelines, para 131.

risks – do recognise that gatekeepers could reasonably take additional steps to verify the trustworthiness of those firms seeking to take advantage of the DMA.

Given the reality that bad actors will (and are) trying to abuse data portability rights, for example through spoofing legitimate services, this approach seems to impose significant reputational risks on gatekeepers and implies very significant levels of trust on data recipients. It is also surprising given that many recipients of data may be outside the EEA (or a jurisdiction the Commission recognises as having an adequate level of data protection) and therefore their level of data protection is unclear. If the only tests the gatekeeper can apply are to check whether an end user has consent to a transfer of data, it is unclear how the gatekeeper will be able to meet the DMA's requirements while also complying with laws relating to cyber security, data protection, consumer protection, product safety and accessibility requirements.

The Draft Guidelines also state that a gatekeeper is not allowed to "restrict, in any way, the data portability use cases and business purposes that authorised third parties can pursue". This seems appropriate since it should be up to the user, not the gatekeeper, to determine which business ideas the user values.

Very similar concerns arise in relation to interoperability, since it can carry high risks to users 'security and privacy and can expose personal data to third party services which may not be trustworthy. In relation to interoperability, the DMA does seek to ensure the obligations still allow gatekeepers to protect users' privacy and security, provided measures are strictly necessary, proportionate and duly justified. [118]

This seems to imply gatekeepers can adopt a balanced approach which does not solely rely on end user consent. This suggests that (unlike with data portability under the proposed Draft Guidelines) a gatekeeper could apply a "screening" process to ensure that software and hardware providers seeking to take advantage of the DMA openness rules are legitimate, good faith actors, who are not misleading or exploiting consumers and with adequate protection of these end users' rights.

The question is how to ensure such mechanisms are proportionate and are not used as a smokescreen to undermine the DMA's objectives. This means measures should be targeted and should not be duplicative. For example, if a gatekeeper adopts an adequate "screening" process for third parties that want to access sensitive functionalities (effectively making a decision for the end user that a developer is "safe"), then there should be no reason for the gatekeeper to then expose the end user to additional warnings implying that they face a lower degree of security or privacy protections. That is particularly the case where (as can sometimes be the case) the third-party service in fact adopts a superior level of security or privacy than the gatekeeper's own service.

It would also be critical that such a "screening" process is not designed in a way which can be misused by the gatekeeper. One way of addressing this issue will be to apply objective objective criteria which can be applied both the gatekeeper and external firms, but which are targeted at specific security concerns rather than gold-plated requirements which only the largest firms can meet. For example, the UK's Open Banking regime sets out specific and verifiable security standards – such as requiring participating firms to meet accepted information security management standards, with firms which

[118] In the DMA, for example, art 6(7) is subject to an exception: a regulated platform is allowed to take "strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features" provided by the regulated platform. Such measures must be "duly justified" by the regulated platform.

fail to comply risking having their regulatory permissions revoked.[119] Under the Open Banking model, a third party (namely the regulator) would decide whether the standards were met. In the DMA, it could be acceptable for the gatekeeper to set and apply the standards (provided they were proportionate, objective and specific). However as noted below, it would be preferable that this function was handed over to a third party, or at least was subject to third party conciliation in the event of a dispute.

3.4 Quality

The quality of the access provided must also be considered. Since the gatekeeper is not required to provide "equivalence of inputs" (that is, it does not need to use the portability and interoperability tools and interfaces it designs for others in its internal workflows), gatekeepers may have an incentive to degrade the quality of the interfaces, make them unstable or subject to continuous change, in order to decrease the ability of third parties to make effective use of them.

In other regulated sectors there are often detailed discussions about service levels – such as the required resilience of a service to unplanned outages, a planned limit on planned outages, and requirements around the timing of delivery of ported data. Similar questions must be addressed in the context of portability and interoperability. The ability for users to multi-home, for example, will be undermined if real-time and continuous portability is not made available. And users may be less likely to use challenger messaging services if the quality of horizontal interoperability – and therefore their ability to communicate with users not using their particular service is haphazard.

The DMA does not set out required quality and service level standards in detail. Portability must simply be provided on a "continuous and real-time" basis. Similarly, the only requirement for vertical interoperability is that it must be "effective". Neither of these terms is defined, creating a question about what standard of access is compliant. Determining the appropriate level of quality implies a trade-off between compliance costs and effectiveness. The Draft Guidelines only state that the data must be "consistently updated, as soon as possible after such information has been provided or generated".[120] Here, work such as BEREC's report on horizontal interoperability highlights the need for minimum criteria on service levels and key performance indicators, and that ideally such criteria would be developed either by a regulator or through an inclusive governance mechanism (explored below).[121]

3.5 Common Implementation Questions

These design questions raise several common implementation issues.

One problem is deciding how expensive implementation should be and how to balance the costs, so that DMA implementation remains proportionate. Some implementation decisions imply greater costs than others, and there may be a trade-off in some cases between cheaper solutions and those which are more effective at achieving the DMA's objectives. There is also a question of how to balance costs – that is, whether more costs should be borne by gatekeepers or by firms trying to take

[119] https://standards.openbanking.org.uk/operational-guidelines/tpp-operational-guidelines/security/v3-1-4/
[120] Draft Guidelines, para 121.
[121] BEREC, 'BEREC report on interoperability of Number-Independent Interpersonal Communication Services (NI-ICS)', 8 June 2023.

advantage of the DMA's rules on openness. Gatekeepers may generally have an interest in making the least possible changes to their pre-existing way of doing business. That may help reduce compliance costs for gatekeepers – but it can also raise costs for business users. Given the diversity and sheer number of different business users which may seek to take advantage of portability and interoperability, and for different purposes, in many cases it does not seem likely that any one single approach will suit all business users. Furthermore, as noted in relation to vertical interoperability, operating systems typically already have well-established APIs which third-party developers can use, and so business users could incur significant costs if gatekeepers changed their approach.

A second problem is how to balance security and privacy with contestability. An unduly strict and precautionary approach to security and privacy might result in little data or functionality being accessible or subject to strict limitations. However, this would undermine the DMA's goals of increasing contestability – and would not likely be necessary, since some gatekeeper platform services are already more open than others without causing an undue level of security concerns. Implementation must be vigilant to ensure security is not used as a smokescreen to undermine the DMA – while also ensuring that properly substantiated security risks are adequately mitigated. The only realistic approach is to seek a proportionate balance between protecting security, on the one hand, and achieving contestability on the other.

A third problem is **how much discretion, subjectivity and flexibility to allow to gatekeepers when designing compliance solutions - and how to balance business users desire for stability, with gatekeepers' interests in maintaining flexibility to innovate**. For a business user to invest in taking advantage of the DMA, they will need to invest in systems that can work with the gatekeepers' interfaces and data formats. This can be a significant investment which would take time to pay off, particularly where a gatekeeper adopts an approach which effectively requires business users to adapt to the gatekeeper's design choices. In those cases, one dilemma is between flexibility and stability. Gatekeepers will want to preserve full flexibility to innovate and evolve their services. If gatekeepers can at any time make changes to their platform in a way which 'breaks' a business user's interoperability or portability tools, then business users will have to continuously make changes to their own services to 'keep up'. This can in turn discourage consumers from trying a challenger service, since there would be no guarantee of seamless connectivity. Some limitations on changes to their platforms will be required (such as notice periods for changes and/or a requirement that changes are made only for genuine reasons) to ensure that interoperability is effective.

Finally, one question is **to what extent all gatekeepers offering the same category of core platform service should adopt the same technical solutions**. The DMA does not require this outcome. Where this is feasible (which might be the case with hardware interoperability, for example, at least over the longer term), it would have advantages for business users. For example:

- a third-party communications service would benefit from being able to seek horizontal interoperability with all gatekeeper messaging platforms using the same processes and APIs; and
- a third-party authorised as a legitimate party to receive ported data from one gatekeeper platform could benefit from being automatically recognised by other platforms. This could have benefits in some cases, but would need to be implemented in a way which takes into account that different gatekeepers might have different standards or trade-offs in terms of

security, based for example on their business model or the type of data/functionality in question.

The DMA recognises that data portability and interoperability can be "facilitated" with the use of technical standards.[122] It envisages that the Commission can request European standardisation bodies to develop appropriate standards.[123] However, it does not mandate that gatekeepers must follow any such standard.

Consistent approaches will not always be desirable (to the extent that differentiation is valued by consumers) and may not be feasible in the short term. For example, for now, gatekeepers have generally adopted their own proprietary interfaces for portability and interoperability. Furthermore, when it comes to data formats, a consistent approach may not be plausible since the obligation covers many different types of core platform services (meaning different data is collected for different purposes). It is also not likely to be possible in the short to medium term for vertical interoperability, given the different software architectures adopted by iOS, Android, and Windows. However, inclusive organisations like the Open Worldwide Application Security Project (OWASP) have developed programs like a security standard for mobile apps, which could be adopted by gatekeepers to at least ensure that elements of their approaches have some consistency,[124] and industry standards exist for hardware functionalities like Bluetooth, even if implementation can sometimes vary. However, a broader attempt at homogeneity would require significant and expensive redesign of these services (with trade-offs for innovation and differentiation). Prematurely enforced standardisation can also 'lock in' particular technical decisions which may prove suboptimal and slow the pace of decision-making.[125] Standardisation can also take a long time and it can be complex to reach consensus among market participants with conflicting incentives. Formal standardisation processes are therefore more likely to be appropriate in contexts where services are relatively mature, the pace of innovation is significantly slower, the number of interested participants is limited, services are less differentiated, and market structures are such that there are no players with outsized importance and there is broad alignment on the merits and opportunities of standardisation. These factors are far more applicable in sectors like electronic communications – where rollout of technologies like 6G require coordination by large numbers of national telecommunications firms – rather than digital platforms.

That does not mean formal standardisation will never be a good option. In particular, as the DMA implicitly recognises, in some markets where there are only one or two large players, the pace of innovation by platforms appears to have slowed, with an increase in innovation taking place in complementary markets (such as between app developers and accessory makers). Furthermore, in many cases the functionality offered by competing platforms is very similar. If this trend continues then the case for standardisation may become stronger over time, particularly in cases where there are already industry standards. However, the shift towards a more institutionalised, inclusive and consensus-driven approach is unlikely to be justified for all gatekeeper core platform services at the same pace.

Even where proprietary approaches are necessary in the short run, in the longer run a more harmonised industry-wide approach should remain an objective for the Commission – with a view to

[122] DMA recital 96.
[123] DMA art 48.
[124] https://mas.owasp.org/.
[125] Chris Riley and James Vasile, 'Interoperability as a Lens onto Regulatory Paradigms', CPI, 2021.

increasing harmonisation over time, particularly in areas where there could be less impact on innovation and competitive differentiation. A priority area might be to adopt common approaches in areas of business processes, commercial terms and setting access criteria – such as when assessing whether a third party is a legitimate recipient of data or functionality. In these cases, consistency could offer a significant way to both lower costs of taking advantage of the DMA for business users. For example, the Data Transfer Initiative's Trust Registry sets out which firms are safe recipients of ported data.[126] CODE also has (as noted above) an 'Ethical Data Badge' initiative which also verifies accredited firms as being trustworthy recipients of data.[127] These offer ways to make the DMA more effective, by giving third parties a 'one stop shop' to becoming accredited to take advantage of the DMA's openness rules. Where similar established, independent, and credible initiatives exist which have cross-industry support, the Commission could encourage gatekeepers to ensure they conform to that body's principles or standards unless there is a good reason not to.

[126] Data Transfer Initiative, 'Update on trust efforts at DTI', 30 July 2024.
[127] Coalition for Online Data Empowerment, https://www.codepolicy.org/.

4. Governance Mechanisms

As the section above has highlighted, the technical and commercial mechanisms which have been put in place in response to the DMA involve many detailed questions – and significant trade-offs. It is clear that gatekeepers have commercial incentives which will not often be fully aligned with the DMA's objectives, but equally that some business users may tend to underplay compliance costs or will understandably seek to push design choices which further their own business models rather than those of end users. Different approaches to making decisions about how gatekeepers comply with the DMA may result in different responses to these trade-offs. A number of different possible approaches – which are not mutually exclusive but aspects of which can be combined – are set out below.

4.1 Gatekeeper-led approaches

The approach taken by gatekeepers to implement the DMA so far has been largely 'top down', with decisions largely being proposed by the gatekeeper and the Commission and third parties largely being consulted. This seems to be the default position envisaged in the DMA. For example, the rules on horizontal interoperability require the gatekeeper to prepare and publish a "reference offer" which business users must accept if they wish to be beneficiaries of horizontal interoperability.

This type of approach reflects today's reality, where many gatekeepers already had tools which largely reflected the DMA's openness objectives. For example, operating systems already have an extensive set of APIs to enable third parties to take advantage of the operating system's functions. Similarly, the gatekeepers already have data portability solutions in place. Google, Meta and Apple have also participated for several years in the Data Transfer Initiative, which aims to provide 'data adapters' so that data from one platform can be 'translated' for use on competing platforms. Given the short timeframe to comply with the DMA, it was understandable that gatekeepers would adopt decisions themselves and with less consultation with other parties than might have been optimal.

One reason for this approach is that the Commission has largely chosen to influence gatekeepers' approaches in a negative form: that is, by either informally signalling that it believes an approach is non-compliant, or by bringing enforcement proceedings against a gatekeeper (but see the discussion of the Commission specifications below). In practice, our understanding of discussions between gatekeepers and the Commission appears to highlight that the Commission is, in effect, supporting a gatekeeper-led approach in most cases, by requiring gatekeepers to proactively propose solutions, and providing limited (and mostly negative) feedback about the merits of those solutions. This has meant, however, that gatekeepers have in several instances rolled out changes even though there is no agreement with the Commission on whether the solution met the requirements of the DMA.[128] In the Commission's second annual report on the DMA, for example, it appears that in a number of cases the approaches taken by gatekeepers are still under review.

A gatekeeper-led approach assumes "corporate capacities to self-regulate"[129] and it has some potential advantages. It may facilitate faster changes within the gatekeepers, since it reduces the need for extensive and time-consuming negotiation with third parties, and therefore allows gatekeepers

[128] BEUC, 'First Bloom: Increased Consumer Choice after Eighteen Months of the DMA', November 2025, p 9.
[129] Robert Baldwin and Martin Cave, 'Taming the Corporation', OUP, 2023, p 6.

maximum opportunity to innovate. It may reduce the costs of compliance for gatekeepers by enabling firms to identify the compliance measures which are most compatible with their existing business models, technical decisions, and organisational processes. And it may maximise the opportunities for gatekeepers to continue to differentiate their approaches on issues like privacy and security.[130]

This type of approach has several disadvantages, however. First, the gatekeeper-led approach provides little predictability for business users and third parties. The Commission, for example, has never declared a gatekeeper to be 'compliant' with the DMA (and it is not even clear whether the Commission has the power to do so). This gives business users little certainty about when a compliance process has reached a relatively stable end-state. This can undermine the case for investing on the basis of DMA compliance tools. The current approach is also likely undesirable for gatekeepers which must continually anticipate the Commission's expectations, and can only infer that they are compliant from the Commission not taking enforcement action or issuing specifications.

Second, it is unclear how well the interests of business users or end users are taken into account when gatekeepers determine their compliance approaches – particularly since gatekeepers do not always have commercial incentives to further the objectives of the DMA. As noted above, implementation involves so many discretionary questions. In that context, allowing gatekeepers to lead the discussion and make decisions on technical mechanisms themselves allows them to act on incentives which might not be fully aligned with the DMA's objectives. For example, in many cases they will genuinely have incentives to keep their platform as open as possible, but in other cases their incentives could be distorted by trying to protect their downstream businesses which could compete with those of business users. This makes it unlikely that decisions made by gatekeepers will always reflect a balanced approach.

Finally, a gatekeeper-led approach provides little reason for gatekeepers to slowly move towards approaches with more industry-wide consistency, which as noted above could have significant benefits for end users.

4.2 A Commission-Led Approach

A second alternative is a regulator-led approach. Under the DMA, the Commission may expressly specify which measures a gatekeeper must take to comply. The Commission issued two such specifications and proposes to issue a third. Gatekeepers may also request that the Commission specify how a gatekeeper should comply with a DMA provision, but no gatekeepers have done so thus far.

This type of approach has some potential advantages:

- It may facilitate faster changes within the gatekeepers and it may help shift gatekeepers away from a minimalist approach to compliance. It has potential to achieve a fairer balance between competing interests – at least insofar as the Commission acts in an impartial way, led by evidence, and objectively weighs different stakeholder interests.
- While the Commission has used this tool by exception in the past, in the future it could use the specification tool to mandate that gatekeepers adopt more consistency in the design

[130] See Zach Meyers, 'Balancing security and contestability in the DMA: the case of app stores' (2024) European Competition Journal.

mechanisms they use (e.g., screening processes for business users).

However, as explained in the previous section, the issues the Commission will need to tackle to make portability and interoperability successful are complex and numerous. It is unlikely that the Commission will have the resources or expertise to address all of them – and certainly not to address all of them well. Therefore, a regulator-led approach is better used as a way to improve legal certainty (where this is necessary) rather than as a first resort to resolve issues.

Furthermore, while a gatekeeper-led approach can be criticised for being insufficiently inclusive, the same may also be true of a Commission-led approach. For one thing, the team in the Commission responsible for enforcing and implementing the DMA are not politically independent in the same way that many other regulators (such as in the electronic communications sector) are. Greater independence would be likely to enhance the legitimacy of DMA implementation, since it would help protect the Commission from perceptions that it has a vested interest in 'acting tough'. Furthermore, the DMA provides few safeguards to ensure that business users' views are taken into account. In practice, when the Commission has specified how gatekeepers should comply, the Commission has done so under significant time pressure. This may have contributed to a perception among some stakeholders that the process proceeds largely through bilateral consultation with the gatekeeper and with other interested parties not being sufficiently heard. Equally, this may result in suboptimal decisions being made which do not pay full regard to risks to security and privacy: as tackling this problem requires deep technical expertise which cannot be acquired overnight. While the specification process has value, a more structured, less time-bound and more inclusive approach could help to ensure the DMA is more effective in the long run.

4.3 Collective and Inclusive Governance Mechanisms

As an alternative to the current gatekeeper-led or Commission-led approaches, gatekeepers could set up more inclusive and collective governance mechanisms. These could aim to create a meaningful dialogue between the gatekeeper, the Commission, businesses which wish to take advantage of the DMA, and potentially other stakeholders like consumer groups.

In theory, this process could have significant advantages – such as enabling many different stakeholders to have a meaningful say on how gatekeepers should become more open, and providing a more clear and transparent process for changing existing openness mechanisms such as APIs. The inclusion of many different stakeholders in the decision-making process can provide greater guarantees that decisions reached will be balanced and that the resulting technical mechanisms will provide a stable, predictable and effective foundation for investment. As noted above, formal standardisation is one option, and while it might be a good approach in some cases (such as where features are already relatively similar across services and the technology is mature) it is unlikely to be the most effective or proportionate in all cases. There are, however, a range of ways to adopt collective and inclusive governance mechanisms without resorting to full standardisation, some of which the Commission appears to be exploring through more multilateral dialogues.[131]

[131] Richard Feasey and Giorgio Monti, 'Implementing the DMA: Early Feedback', CERRE, March 2025, p 15.

There are a number of practical difficulties that would need to be overcome in the design of such collective and inclusive governance mechanisms, however.

The first is defining the participants. Unlike in many other regulated sectors with portability and interoperability rules, such as energy or banking, there is no licensing or authorisation process or qualifying criteria before a business can take advantage of the portability or interoperability rules in the DMA – and the number of interested parties is potentially extremely broad. The mobile app ecosystem, for example, each have millions of registered app developers.[132] Furthermore, decisions should be made not only taking into account the views of existing access seekers (such as those who have signed developer agreements with operating system providers), but also the interests of future access seekers who might launch innovative new business ideas. There may be a risk that an inclusive process gives too much weight to the interests of a minority of business users with narrow interests, whereas an inclusive process ought to include a broad cross-section of stakeholders.

The second is how decision-making should be made. Experience in other regulated sectors with inclusive governance mechanisms illustrates that consensus can often be very difficult to achieve, even when the business models which regulation is trying to unlock (such as telephone number portability, or allowing third party payments) are clear and well-understood. Agreement is likely to be much harder to achieve in relation to portability and interoperability where different business users have very different priorities, interests and business ideas they wish to pursue – and where some ideas will clearly have much more consumer benefits than others. Identifying a way to balance these interests will be far from trivial.

A third and related point is how to ensure speed of decision-making is sufficient. Existing standard-setting processes are notoriously slow, even when dealing with relatively mature technologies. While Europe's standard-setting bodies have been working hard to develop AI standards in time for the implementation deadline of most of the AI Act, for example, they have been unable to prepare standards in time. This problem is likely to be even greater where different stakeholders have significantly different interests at stake.

Finally, collective decision-making has important implications for the pace and direction of innovation. Many innovations or decisions about platform governance will have winners and losers. Platform operators may therefore play a "system orchestrator" role - facilitating innovation by centralising decision-making and deciding which innovations to prioritise.[133] Even if this might not deliver the highest-value innovation, it might be preferable to an approach where development slows significantly because of the inability to obtain consensus.

One option might be for key decisions about how to design an inclusive and balanced process to be 'outsourced' to a regulator or independent expert, who could then design a process which balanced the needs of different stakeholders.

[132] Furthermore, while the gatekeepers may impose access criteria, since those criteria would be a potential subject of discussion in the governance forum, firms should not be excluded simply because they do not meet the existing criteria.

[133] Anssi Smedlund and Hoda Faghankhani, 'Platform Orchestration for Efficiency, Development, and Innovation', IEEE, 2015, https://ieeexplore.ieee.org/document/7069977/.

4.4 Third-Party Mechanisms

As noted above, the fundamental problem with gatekeepers making decisions themselves is their conflict of interest: while in many cases they will genuinely have incentives to keep their platform as open as possible, in other cases their incentives could be distorted by trying to protect their downstream businesses which could compete with those of business users. A Commission-led approach and a more inclusive governance model each have their own weaknesses.

One governance solution which should be introduced is that, instead of giving the Commission a broad approach in leading the agenda on implementation, it – or an independent third party trusted by both business users and gatekeepers – could adopt a narrower approach. As noted above, this narrower role could be to design an inclusive governance process, but it could also involve directly deciding some issues, particularly where there is a dispute or impasse. In other regulated sectors, this role can be undertaken by a regulator: for example, in the electronic communications sector, disputes between access seekers and gatekeepers can be referred to the regulator for arbitration. National regulators are required to arbitrate disputes between incumbent firms and access seekers 'in the shortest possible time-frame' and (normally) within four months.[134] However, the Commission lacks the institutional independence of national electronic communications regulators. Furthermore, given the complexity of the issues and the number of potential disputes, it is unlikely that the Commission would be in a position to adjudicate all possible disputes. Therefore, an independent third party may provide a better solution.

The Commission has required one gatekeeper to adopt a non-binding 'conciliation' process where there is a dispute, by having an independent expert provide a view about any technical disputes.[135] Similarly, in the Epic Games v Google litigation in the US, the judge appointed a three-person 'Technical Committee' to solve any implementation disputes. Another example is when the UK implemented Open Banking: the law provided for an 'Open Banking Implementation Entity' which could impose solutions on the parties when there was no agreement. Recourse to a regulator is a well-used mechanism in regulation, however experience in other sectors suggests it is important that such as conciliator is genuinely independent and properly empowered rather than merely advisory. While there is a risk that a conciliator role would create legal uncertainty (because a court may ultimately disagree with the conciliator) this risk is minimised if the conciliator's role is limited to highly technical matters. Because the intervention of a third party imposes some uncertainty on the ultimate outcome, it tends to incentivise parties to take reasonable positions and seek consensus where possible. A conciliation process would need to be designed in a way which ensures it is accessible to smaller stakeholders, while also ensuring it is not used vexatiously or in a way that allows competitors or malicious actors to unreasonably tie up the gatekeeper's resources or its pace of innovation.

One important benefit of third-party mechanisms is that, at least on some issues, they can be applied across industry – promoting more consistency and predictability for business users which may need to seek data portability or interoperability across multiple platforms or operating systems. Complete consistency, especially at a technical level, is unlikely to be proportionate. However, there is likely to be a degree of commonality on certain questions, such as how to authenticate a user and whether a particular business user is a legitimate recipient of data or access to system functionality. As noted

[134] European Electronic Communications Code, Directive (EU) 2018/1972, art 26.
[135] https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100204_2073.pdf

above, the Data Transfer Initiative's Trust Registry – which sets out which firms are safe recipients of ported data[136] and has participation from several gatekeepers – offers a promising example for how such a system could work. The initiative operates akin to the 'country of origin' principle: allowing a firm which has been authorised by one participating data holder to receive data from any other participating data holder. This offers an elegant solution to minimising conflicts of interest, since a business user will not then have to individually seek authorisation from each gatekeeper it wishes to obtain data from.

4.5 Incentives and Institutions for Better Governance

In other regulated sectors where collective and inclusive governance has emerged, this has been the result of creating both the right institutions - and the right incentives for both gatekeepers and access seekers to participate. In sectors like telecoms and banking, collective portability and interoperability regimes have emerged with a reasonable degree of success.

In relation to **institutions**, the DMA does not envisage any institution or forum to act as a forum for dialogue between business users, consumers and gatekeepers. Instead, the only mechanism referred to is the use of industry standards. However, as noted above, standard-setting is a slow process and is unlikely to be a suitable way to reflect gatekeepers' legitimate interests in flexibility and ability to innovate in all cases. Furthermore, standards usually involve industry-wide approaches – and while there may be benefits in trying to develop more industry-wide consistency, it is far from clear that this would be a proportionate approach in relation to (say) vertical interoperability given that different operating systems would need significant re-engineering to be able to provide exactly the same technical solutions for business users.

A better institutional approach might be to set up a bespoke forum (or forums) for DMA implementation issues, along the lines of the many similar models which exist in the telecommunications and energy sectors, and during the creation of Open Banking. In the short term, however, the Commission could aim to encourage gatekeepers to adapt their current approaches to compliance in ways which reflect some of the benefits of more open, inclusive approaches. This could include, for example, encouraging gatekeepers to:

- Provide greater transparency – such as documenting (where proportionate) which functionalities are available to access under the DMA rather than business users trying to identify these and which data is available for porting. The Draft Guidelines indicate that "gatekeepers should keep an internal list of all categories of data that can be ported" and there is no reason this could not be published.[137] Furthermore, gatekeepers could provide more clarity about the way in which (and the timeframes with which) decisions about access are decided;
- Set up standing forums and dialogue with business users, which should meet regularly and be attended by representatives of the Commission. However, there is a general agreement among many stakeholders that public workshops may not be the most effective way of driving

[136] Data Transfer Initiative, 'Update on trust efforts at DTI', 30 July 2024.
[137] Guidelines, para 111.

consensus and encouraging open exploration of issues and possible solutions. Other formats such as private workshops might be explored as alternatives. The forums should also engage relevant agencies such data protection, cybersecurity and consumer protection bodies;

- Provide certainty about the stability of technical mechanisms and how they might change in future, including providing a reasonable notice period before changes are made which break existing technical mechanisms or require changes by access seekers. Caution would need to be exercised, however, as this should not result in gatekeepers being required to disclose competitively sensitive information, such as about future product launches;
- Either document clear, objective criteria for how access decisions will be made, which minimise the need for subjective and discretionary judgements, or allow recourse to neutral, independent third parties; and
- Participate in initiatives from trusted and independent third party intermediaries – which can help preserve a platform's ability to innovate and evolve, while meaning business users do not always have to make 'catch up' investments to keep portability and interoperability functional. This suggests the Commission should encourage gatekeepers to support and facilitate the use of 'data adapters' like the Data Transfer Initiative (DTI)[138] which can 'translate' data from one service so that it is (at least to some extent) readable by the recipient service.

In relation to **incentives**, the Commission should consider a combination of 'carrot and stick'. The Commission needs to adopt practices to incentivise gatekeepers to engage in dialogue. These could include, for example:

- signalling that it will take broad industry consensus, or good evidence of a bona fide attempt to understand and balance the views of different stakeholders, as a strong indicator of compliance;
- taking a similar approach of encouraging gatekeepers who adopt APIs and data formats which adhere to accepted industry standards, and indicating these are unlikely to be challenged as non-compliant; or
- scrutinising more closely those gatekeepers whose approaches have been decided without much evidence of consultation or of genuinely reflecting the DMA's objectives.

Importantly, such incentives do not need to necessarily drive gatekeepers towards one particular compliance approach. But they could send clear signals about the range of approaches which would be proportionate: for example, that relying on both certification of access seekers and warning screens for end-users would be more carefully scrutinised than gatekeepers who chose to rely on just one of those mechanisms.

As CERRE has noted previously, **more open governance could help create a culture of 'shared responsibility for managing the risks of data portability and vertical interoperability**.[139] Currently, putting the sole responsibility for designing compliance solutions on gatekeepers means that they may, rightly, want to minimise any risk of negative consequences they would be held accountable for.

[138] https://dtinit.org/.
[139] Zach Meyers, 'Which Governance Mechanisms for Open Tech Platforms?', CERRE, January 2025.

Moving away from this risk-intolerant approach would, however, require close engagement within different parts of the Commission (such as between DMA enforcers and cybersecurity experts in DG-CONNECT) and with other bodies such as data protection and cyber security regulators. This could help ensure outcomes are balanced, take risk into account, reflect the different objectives which EU law tries to further, and help provide assurances to gatekeepers, business users and enforcement bodies about how the risks of openness can be fairly managed and allocated. Regulators and business users would need to propose proactive and reasonable solutions, and to accept a degree of responsibility if those solutions are adopted and risks materialise. Such 'shared responsibility' approach should reduce the incentives for gatekeepers to adopt a cautious approach to managing the risks of openness.

5. Conclusions and Recommendations

Far from being a self-executing law, implementation of the DMA has proven to involve complex technical questions for gatekeepers – particularly in the context of mandating greater openness, which requires careful attention to how to protect service integrity, security and privacy. In this context, the current approach to implementation – with the Commission only targeting selected areas of alleged non-compliance, and gatekeepers largely deciding compliance mechanisms themselves, except in the cases where the Commission has specified that a gatekeeper must take a particular approach – is unlikely to result in balanced outcomes. It provides too much discretion to gatekeepers – providing less certainty and predictability for business users and allowing too much scope to use commercial and technological implementation decisions to undermine the effectiveness of portability and interoperability rules. The most optimal solutions to DMA compliance are likely to emerge through open governance processes where the various trade-offs can be thoughtfully and conscientiously considered.

Rather than intervening in more cases, a focus on improving governance mechanisms might prove a more efficient way to make the DMA more effective in the long run. Full standardisation of compliance mechanisms is unlikely to be proportionate in every case, but a shift towards more inclusive, predictable ways of developing and updating compliance solutions would likely produce better outcomes – as would a more sector-wide approach to some compliance questions. Openness may help gatekeepers and business users 'show their hands'on many issues up-front so that any disputes can be identified and tackled quickly and simultaneously. To do this, the Commission could evolve its approach to provide clearer incentives for gatekeepers to adopt inclusive and open governance mechanisms.

DMA Regulatory Interplays

Alexandre de Streel
Giorgio Monti

1. Coherence of the EU Digital Rulebook

1.1. The importance of regulatory consistency

The interplay between the Digital Markets Act (DMA) and the other EU and national legal frameworks applicable to DMA designated gatekeepers and benefiting business users has become an increasingly salient issue as DMA enforcement advances. **As concrete cases emerge, a range of trade-offs between the different rights, objectives, and interests protected by distinct legal instruments which were left unresolved by the EU legislator are now becoming more visible.** If left insufficiently addressed, these tensions risk undermining regulatory predictability, legal certainty, and consistency across the EU digital rulebook. This challenge is particularly acute in the current policy context, as the EU seeks to boost productivity and regain global competitiveness, with the digital sector widely recognised as a key engine of growth and innovation.[140]

In its recent Report on the interaction between the Digital Services Act (DSA) and 54 other EU legal acts, the European Commission observed that: [141]

> *"The (stakeholders) surveys highlight a broad consensus on the need for clarity, coherence, and coordination within the Union's digital regulatory landscape. (…) To ensure effective enforcement, protection of users, and a level playing field for businesses, stakeholders call for streamlined guidance, better institutional cooperation, and practical tools that make the regulatory framework more accessible and predictable."*

These observations apply with equal force to the interaction between the DMA and other areas of EU law. So far, the most discussed DMA interplays relate to competition law (as the DMA was partly based on antitrust cases), privacy rules (as we explained in section 2) and cybersecurity rules.[142] However, several other regulatory interplays are key for an effective and proportionate implementation of the DMA, in particular with the DSA or the IP rules.

The Interplay with Digital Services Act

The DMA and the DSA form two complementary pillars of the EU digital rulebook. Although the two instruments pursue distinct objectives—contestability and fairness in the case of the DMA, and safety, transparency, and accountability in the case of the DSA—they apply to overlapping categories of large digital service providers. As such, they should be understood not as isolated regimes, but as interlocking components of a broader regulatory framework. The DMA seeks to prevent entrenched gatekeepers from leveraging their intermediation power to distort competition and stifle innovation. The DSA, by contrast, aims to mitigate systemic risks related to illegal content, disinformation, fundamental rights violations, and societal harms arising from the functioning of online platforms. Despite these different focal points, **both regulations share several underlying principles**, such as increasing transparency of platform practices, reducing information asymmetries, enhancing

[140] Draghi M. (2024), The future of European competitiveness; Part B: In-depth analysis and recommendations, Report to the Commission.
[141] Report from the Commission of 17 November 2025 on the application of Article 33 of Regulation 2022/2065 and the interaction of that Regulation with other legal acts, COM(2025) 708, p.10.
[142] Those interplays were already discussed in last year CERRE DMA Report: https://cerre.eu/publications/dma-implementation-forum/

accountability of large digital intermediaries, and protecting users (both business users and end users) from unfair or harmful practices. In this sense, the DMA and DSA can be seen as two sides of the same coin: one addressing market structure and economic power, the other addressing systemic risks and societal impact.

Several areas offer clear opportunities for coherent and mutually reinforcing implementation.

- **Transparency of rankings and recommender systems:** the DMA requires gatekeepers to ensure transparency in ranking practices, particularly where self-preferencing or discriminatory treatment may distort competition. The DSA, in turn, imposes transparency obligations concerning recommender systems, including the main parameters used and the options available to users to modify or influence those systems. A coordinated interpretation of these provisions can enhance both economic fairness and user autonomy. Greater transparency in ranking and recommender systems can enable business users to compete on more equal terms (DMA objective), empower users to understand and control how content is curated and prioritised (DSA objective), and facilitate regulatory oversight by reducing informational asymmetries. Ensuring consistency in technical and disclosure standards across both instruments would reduce compliance complexity while strengthening regulatory effectiveness.
- **Harmful online choice architecture (dark patterns):** the DSA contains explicit provisions addressing manipulative or deceptive interface designs that distort user decision-making. The DMA addresses unfair practices imposed by gatekeepers on business users and end users, including restrictions on switching, steering, or interoperability. There is clear potential for synergy: manipulative interface design can both harm users (a DSA concern) and entrench gatekeeper power by increasing switching costs or limiting effective multi-homing (a DMA concern). Coordinated enforcement could ensure that interventions targeting dark patterns also support broader contestability goals.
- **Online advertising:** the DMA includes obligations on online ad transparency and concerning data combination and restrictions on leveraging user data across services without consent, thereby targeting competitive advantages derived from data accumulation. The DSA establishes transparency obligations for online advertising, including disclosures about targeting criteria and advertiser identity. Together, these measures can increase transparency in digital advertising markets, reduce exploitative or opaque targeting practices, limit the entrenchment of data-driven market power, and strengthen user trust and accountability.

To avoid fragmentation or inconsistent interpretations, **enforcement actions should consider the cumulative impact of obligations under both regimes**. Moreover, evidence gathered in DSA systemic risk assessments could inform DMA investigations into market practices and remedies under one framework should not undermine objectives pursued under the other.

Moreover, while synergies are significant, care must also be taken to avoid duplicative or conflicting obligations. Clear guidance should delineate where obligations pursue distinct objectives and where they overlap substantively. Legal certainty is particularly important for platforms subject to extensive reporting, auditing, and transparency requirements under both regimes. A coherent interpretative framework should aim to align definitions and technical standards where feasible, clarify the

interaction between transparency obligations and ensure proportionality in cumulative compliance burdens.

The Interplay with IP rights

IP protection constitutes a fundamental component of the European Union's legal order. The right to intellectual property is explicitly protected under Article 17(2) of the EU Charter of Fundamental Rights and is further embedded in international agreements such as the TRIPS Agreement. The rationale underpinning IP protection is well established: by granting exclusive rights to inventors and creators—including those responsible for the diffusion and commercialisation of innovations—IP law seeks to incentivise investment in research, development, and creative production. Therefore, **there is no inherent conflict between the objectives of IP law and the DMA as both regulatory frameworks ultimately pursue innovation**. IP law does so by rewarding and protecting inventive and creative efforts, while the DMA seeks to preserve contestability and fairness in digital markets, thereby ensuring that innovation is not stifled by entrenched gatekeeper power. In principle, competitive digital markets and robust IP protection are mutually reinforcing.

However, **tensions may arise in practice**. Certain DMA obligations—such as interoperability requirements or data access mandates —may intersect with protected IP rights, including patents, copyright in software or database rights.[143] In such situations, two analytical steps are crucial.

First, it is essential to clearly **identify the policy choice made by the EU legislator** when adopting the DMA. Where the DMA imposes specific obligations that potentially intersect with IP rights, this reflects a conscious legislative balancing between market contestability and exclusivity-based incentives. Importantly, the recognition of IP as a fundamental right does not render it absolute. Under EU law, fundamental rights—including property rights—may be subject to limitations, provided that such limitations are provided for by law, respect the essence of the right, pursue objectives of general interest recognised by the EU, and comply with the principle of proportionality. The DMA itself embodies a legislative determination that ensuring fair and contestable digital markets constitutes an objective of general interest of high importance within the internal market.

Second, in **implementing and enforcing the DMA, authorities—primarily the European Commission—must apply its provisions in an effective and proportionate manner**, in line with the general principles of EU law and the Charter. This entails a necessity assessment as the DMA obligations that intersect with IP should be effective enough and go no further than necessary to achieve contestability and fairness; this implementation is context-sensitive as enforcement decisions should carefully distinguish between legitimate exercises of IP rights and strategic uses of IP to entrench gatekeeper power. A rigid or overly expansive interpretation of DMA obligations could risk undermining the incentive structures that IP law seeks to preserve. Conversely, an overly deferential approach toward IP claims could frustrate the DMA's core objective of reducing structural barriers to entry and expansion in digital markets.

To ensure legal certainty and coherence, policymakers and enforcement authorities should articulate a **structured framework** clarifying how possible specific and substantiated IP claims could be assessed

[143] For example, interoperability mandates could require gatekeepers to provide access to interfaces or technical information that is otherwise protected under IP regimes. Similarly, data portability and access provisions may raise concerns where datasets are subject to copyright or database protection.

in DMA proceedings. Such a framework could require gatekeepers invoking IP protection to substantiate the scope and necessity of the claimed exclusivity, and for the Commission to assess whether the IP right is being exercised in a manner consistent with its essential function, evaluate whether equally effective and less restrictive alternatives are available and consider the long-term dynamic effects on innovation, both at the level of the gatekeeper and for third-party market participants. By making the balancing exercise transparent and predictable, the EU can reduce legal uncertainty and mitigate litigation risks while preserving both innovation incentives and competitive market structures.

1.2. How to achieve regulatory consistency

To manage and rationalise regulatory interdependencies within the EU digital acquis, there are several legal and institutional mechanisms.

First, the **Commission could adopt interpretative guidelines—potentially developed jointly with other EU institutions and bodies—to clarify the interaction between different legislative instruments**. The joint Commission–European Data Protection Board (EDPB) Guidelines on the interplay between the DMA and the GDPR is the first example of this approach;[144]

This first strategy, which remains at an early stage, is particularly valuable insofar as it has the potential to enhance regulatory predictability and consistency in a flexible manner and without reopening long and complex legislative negotiations. But because soft law does not change hard law, it is always without prejudice of the interpretation of the legal text by the Courts. We discuss in more detail the draft Joint Guidelines on DMA-GDPR in the next section. At this stage, suffice it to say that the process for adopting those joint guidelines should be transparent and participatory involving all the stakeholders. Equally important, the outcome should not amount to a mere aggregation of institutional, legal or policy positions. Rather, it should constitute a coherent piece of soft law that clearly identifies how synergies between the respective legal frameworks can be maximised, how tensions can be mitigated, and how unavoidable trade-offs can be resolved in practice.

Second, the **Commission has initiated a process of legislative simplification through so-called omnibus proposals**. To date, three such proposals have been tabled with a view to simplifying the EU digital acquis: two primarily addressing data-related legislation, and a one focused on artificial intelligence.[145]

This second strategy seeks to rationalise the EU digital rulebook by removing or consolidating overlapping regulatory obligations. A prominent example is the Digital Omnibus proposal of November 2025, which includes a proposal to repeal the Platform-to-Business (P2B) Fairness Regulation.[146] To the extent that the DMA already contains a range of obligations designed to ensure fairness in platform-to-business relations for gatekeepers, this repeal may be justified. Moreover, while the DMA and the DSA introduce asymmetrical regulation targeted at platforms with significant market power, the P2B Fairness Regulation applied horizontally to all platforms, regardless of their

[144] EC-EDPB Joint draft Guidelines of October 2025 on the interplay between the DMA and the GDPR.
[145] COM (2025)501 and COM(2025) 837 for data; COM(2025) 836 for AI.
[146] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ [2019] L 186/55.

economic position. From this perspective, its repeal can be seen as a correction of regulatory overreach, with the potential benefit of alleviating compliance burdens for smaller platforms.

At the same time, several substantive elements of the P2B Fairness Regulation could usefully inform DMA implementation through guidance. For example, Article 5 of the P2B Regulation and the associated guidelines,[147] which establishes transparency requirements regarding the ranking of search results vis-à-vis business users, could provide a helpful interpretative framework for compliance with Article 6(5) DMA. Similarly, Articles 11 to 13 on internal complaint-handling systems and alternative dispute resolution mechanisms could serve as reference points for designing effective and proportionate dispute resolution frameworks for gatekeepers under the DMA.

In addition, a future omnibus proposal could be tabled to strengthen both the legal capacity and the incentives for cooperation among the EU and national regulators responsible for enforcing the digital acquis—numbering more than 270,[148] according to the Draghi Report. As discussed in Section 3, this would entail the establishment of a dedicated secretariat to support such cooperation, as well as the introduction of mechanisms allowing for the exchange of confidential information.

Third, the **Commission has announced a "digital fitness check" intended to assess how different elements of the EU digital rulebook operate in combination**. This exercise aims to identify synergies and good practices, as well as remaining gaps, overlaps, and inconsistencies—both at the substantive and institutional levels.[149]

This third strategy has the potential to support the most ambitious reforms, as it could enable a more systematic streamlining of the EU digital rulebook at both the substantive and institutional levels. For this exercise to be effective, however, the Commission will need to engage in a more explicit and rigorous analysis of the trade-offs between overlapping legal regimes and the interests they protect.[150] This, in turn, requires a robust, evidence-based evaluation of the core instruments of the digital rulebook, including the DMA. In a companion issue paper on the impact of the DMA, we therefore call for the development of a dedicated evaluation framework tailored to the DMA's objectives and enforcement mechanisms, as well as for the systematic collection of relevant empirical data.

[147] Commission Guidelines of 7 December 2020 on ranking transparency pursuant to Regulation 2019/1150 of the European Parliament and of the Council, OJ [2020] C 424/1.
[148] Draghi Report, Part A, p.26.
[149] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.
[150] M. Bassini, M. Maggiolino and A de Streel, Better Regulation and Evaluation for the EU Digital Rulebook, CERRE Report, 2025: https://cerre.eu/publications/better-law-making-and-evaluation-for-the-eu-digital-rulebook/

2. Interplay with Data Protection Law

While we have commented on the relationship between the GDPR and the DMA in earlier reports,[151] this issue remains controversial and unresolved and there has been more activity in this policy space that affects how the DMA and the GDPR interact. Below, we discuss three developments. As with previous reports, **we do not discuss whether gatekeepers comply with EU Law. We identify legal and policy issues that affect the interpretation of the rules and the expected impact of the DMA** and make policy recommendations.

The documents discussed below rightly underscore the point that the **relationship between DMA and GDPR is not one whereby the former is a *lex specialis* to the latter.[152] Rather, the two Regulations must be read in a manner that enables the party subject to both obligations to comply with these in a coherent manner**. This is an important observation which should be set out regularly as many still argue that the lex specialis argument has a role to play. This is not the case here for two reasons. First, because the DMA explicitly limits the gatekeeper's entitlement to rely on certain legal bases of the GDPR to process data. Thus, there is no need to invoke a legal doctrine of lex specialis because the DMA provides for an explicit qualification of the GDPR when gatekeepers comply with Article 5(2) DMA. For all other provisions of the DMA, the GDPR applies in parallel and without modification. Second, because when consent is used as a legal basis in the DMA, then the gatekeeper must comply with both DMA and GDPR. That the DMA adds certain requirements in a specific instance does not turn it into a lex specialis.

2.1 Pay or consent models

On 17 April 2024 the European Data Protection Board issued an Opinion on consent or pay models.[153] This Opinion is limited to interpreting the GDPR considering recent case-law, notably the *Meta* judgment.[154] However, the EDPB has interpreted it in a way that in its view aligns with the DMA to ensure a coherent application.

The EDPB takes a restrictive reading of the ability of a large online platform to rely on a consent or pay model where the end user is presented only with an option to consent to personal data collection or to pay for the service and have no data collected.[155] It reiterates the view that 'personal data cannot be considered a tradeable commodity.'[156] However, this position is weakened by the advice it sets out, which is that the platform has to provide the end user with a third option which is free of charge, without behavioural advertising but with a form of advertising which involves the processing of less personal data. In other words, the **EDPB foresees a three-tiered choice architecture**: (i) pay to have a service where no personal data is collected save what is strictly needed to run the service; (ii) a free version with less personal data collection which provides equivalent services to the end user if they share more data, where consent is needed; (iii) a free version with more personal data collection. The

[151] A. de Streel, R. Feasey and G. Monti, *DMA@1: Looking Back and Ahead*, CERRE report, 2025: https://cerre.eu/publications/dma-implementation-forum/.
[152] The doctrine of *lex specialis derogat legi generali* stands for the proposition that that a more specific legal provision should take precedence over a more general one when the two laws are in conflict.
[153] EDPB Opinion 08/2024 of 17 April 2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.
[154] Case C-252/21 *Meta Platforms v Bundeskartellamt* EU:C:2023:537.
[155] In contrast the ICO in the UK takes a more permissive stance. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/consent-or-pay/about-this-guidance/.
[156] EDPB Opinion 08/2024, para 180.

three-tiered option is one that appears to align with DMA recitals suggesting that end-users should be offered with a 'less-personalised but equivalent alternative.'[157] Irrespective of the merits of this approach to DMA compliance, it is hard to see how one can insist that personal data is not traded when end users are making a choice about how much data to reveal (and thus to trade) in exchange for the service.

What the EDPB Opinion is also weak on is the **design of choice architecture**, an issue which instead has been dealt with in part by the Italian competition authority (Autoritá Garante della Concorrenza e del Mercato, AGCM) in a commitment decision relating to Google using its consumer law powers, where the concern was that end-users were nudged to agree to more data collection and processing rather than to make choices to limit this.[158] We will discuss this case further later regarding its significance for inter-agency cooperation (see section 3). For now, it offers a useful case study on the importance of regulatory involvement in choice architecture.[159]

On substance, the AGCM's commitment decision means that Google will change its consent requests allowing users to understand more fully the implications of consenting to the use of personal data. It also provides that the user can limit consent only for certain services and does not expect a degradation of service if this choice is made. The commitment decision contains infographics to illustrate the choice screens and how Google plans to amend them. While a market test was carried out, it remains puzzling to us why the firm is not required to provide any evidence of having tested these choice screens and explaining why it considers these changes are effective. The screens are **tested by the AGCM for legal compliance,[160] but they are not tested for their effectiveness** in achieving the goal of the law, in this case consumer protection.[161] For example, it is assumed that sending an email to users about their choices and their impacts is suitable to repair any harm caused by previous choice options.[162] No evidence is used to determine if this is likely to be the effect of this measure. The design of choice screens is key for many obligations in the DMA and further efforts are needed to identify best practices.[163]

2.2 Joint Guidelines DMA/GDPR

The draft Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation were issued by the Commission and the EDPB on 9 October 2025 and were opened for comment until 4 December 2025.[164] At the time of writing responses are unavailable; below we provide our assessment.

[157] DMA, Recital 36. Meta's alignment with this is presently under review: Commission finds Apple and Meta in breach of the Digital Markets Act Press Release IP/25/1085 (23 April 2025).
[158] Case PS12714 (4 November 2025).
[159] A. Fletcher, 'Choice Architecture for End Users in the DMA' (CERRE, 2023), A. Fletcher and Z. Vasas, 'Implications of Behavioural Economics for the Pro-competitive Regulation of Digital Platforms (2025) 40 Oxford Review of Economic Policy 808.
[160] Case PS12714, section VII.
[161] On choice archicture and consumer protection, see C. Busch, A. Fletcher and M. Ledger, Towards an EU Consumer Law Fit for the Digital Age, CERRE Report, February 2026.
[162] Case PS12714 para 39.
[163] See for instance, https://research.mozilla.org/browser-competition/choicescreen/.
[164] Draft available at: https://www.edpb.europa.eu/news/news/2025/dma-and-gdpr-edpb-and-european-commission-endorse-joint-guidelines-clarify-common_en.

2.2.1 Trade-offs and cooperation between gatekeepers and business users

The draft, as the Opinion discussed above, explains that the **DMA and the GDPR should be interpreted in a comparable manner so that the objectives of both can be met**. However, we see that this is frequently challenging because the business models of some gatekeepers are based on extensive collection and processing of personal data. On the one hand, we agree that excessive collection and processing of personal data with weak or non-existent consent functionalities is harmful for end users. On the other hand, advertising-based business models provide end users with many valuable services and benefit small traders who can advertise effectively.[165] The DMA and competition law seek to make markets where this business model is prominent, as well as related ad tech markets, more contestable.[166] Similarly, while respect for personal data protection is vital, access to data is essential to stimulate competition in search markets and it has been argued that restrictive interpretation of anonymisation can create entry barriers that undermine the market opening effects of Article 6(11) of the DMA.[167] There are thus a number of **trade-offs to be addressed** by the regulators.

Moreover, examples would be particularly helpful in situations where gatekeepers' compliance requires that they cooperate with business users. Guidelines should help gatekeepers and business users understand their obligations and their rights under the DMA and under the GDPR. As long as they comply with both laws, gatekeepers remain free to differentiate their business models according to the level of privacy protection they offer. Some examples from the draft are selected below to illustrate the need for gatekeeper-business user cooperation in ensuring compliance with the DMA and therefore the **need of robust governance mechanisms** as explained in the companion paper on governance as a personal data breach caused by a business user can be a reputational risk for the gatekeepers.

- When it comes to Article 6(4) DMA, both gatekeepers and app developers are separate controllers, so both must comply with GDPR. The draft guidelines recognise that some coordination is needed, for example gatekeepers should avoid designing technical measures or entering into agreements that prescribe the way the app developer chooses to comply with the GDPR.[168]
- Under Article 6(4) DMA, in cases where there is a data breach, appropriate means for handling this jointly or alone are needed so that both parties comply with Articles 33 and 34 GDPR.[169]
- When the app store or app provider must seek consent to process personal data, the gatekeeper must enable them to provide interfaces with prompts for consumers. Gatekeepers may offer some services to help developers, but the latter should remain free to select their own approach to GDPR compliance.[170]
- When data portability processes start (Article 6(9) DMA), both gatekeeper and the business that receive the ported data must comply with GDPR and the gatekeeper has to provide

[165] https://www.tse-fr.eu/sites/default/files/TSE/documents/sem2024/eco_platforms/aridor_juin_2024.pdf.
[166] See e.g. AGCM, App Tracking Transparency (16 December 2025). An executive summary is available here: https://en.agcm.it/dotcmsdoc/pressrelease/A561_SUMMARY.pdf. The AGCM does not question the legitimacy of the business model.
[167] See https://prufer.net/wp-content/uploads/2025/12/consultation-response-on-the-ec-edpb-draft-guidelines-jp.pdf.
[168] Para 93.
[169] Para 97.
[170] Paras 100-101.

appropriate information about the recipients to the data subject. It may also have to provide the data recipient with tools to exclude from the dataset the personal data of individuals other than the end-user seeking portability.[171]

- Article 6(10) DMA compliance requires that gatekeepers allow business users to obtain the consent of end users for access to their personal data. The guidelines recognise that cooperation is needed so that gatekeepers facilitate this while recalling that GDPR compliance obligations vest on the business user as well.[172]

In all these instances, effective workflows are necessary for business users understand what options are available and what they can expect from gatekeepers and what technical options are available to them to both avail themselves of the DMA rights and comply with the GDPR. Any guide that facilitates cooperation will make entry more effective. Some of the workflow could be tested either by the Commission or in a consultation with business users and gatekeepers. Going even further, we can envisage that the workflow following those guidelines would be presumed to comply with the DMA if it is approved; this kind of safe harbour helps with planning and can lead to quicker compliance.

On pay or consent, the draft guidelines are aligned with the earlier EDPB Opinion and focus on the importance of '**user-friendly choices and consent designs**.'[173] However, this is a complex exercise since the guidelines explain that there there should be a separate opt-in for each purpose e.g., personalisation of content, personalisation of advertisements, and service development are three different purposes and a separate consent moment is required for each.[174] As we have explained in earlier reports and above, more efforts should be devoted to **designing choice architecture that allows end-users to understand what they are agreeing to**.[175] The DMA places an obligation on gatekeepers to demonstrate compliance (the same obligation is found in the GDPR[176]) and priority should be placed on requiring gatekeepers to explain why certain choice architecture has been selected, what kind of testing has been carried out.

Here also, a **multi-party regulatory dialogue - supported by robust governance mechanisms - may be of assistance** to develop a common understanding about appropriate choice architecture. In the medium term, arriving at a common understanding can reduce compliance costs and make choice easier for consumers if choice design is similar across all platforms.

2.2.2 Nudging compliance design

An interesting feature of the draft guidelines are instances where the document provides indications about **how a gatekeeper demonstrates compliance. These are framed as desirable types of conduct** (what a gatekeeper 'should' do). Here are some examples:

- Art 6(4) DMA allows gatekeepers to take steps to protect the integrity of hardware or operating systems as well as the security of end users. The draft guidelines advise that

[171] Paras 113-114.
[172] Paras 160-164.
[173] Ibid., Para 19 and section 2.3.
[174] Ibid., paras 30 and 31.
[175] https://cerre.eu/publications/dma-implementation-forum/.
[176] GDPR, Article 24, which reads "… the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

gatekeepers should keep a list of the measures put in place and for each explain the applicable provisions of EU Law as well as the rationale justifying why there are no other effective means to comply with these legal requirements;[177]

- With data portability under Art 6(9) DMA, the guidelines provide that gatekeepers should keep an internal list of all categories of data that can be ported;[178]
- Similarly, with art 6(10) gatekeepers are encouraged to keep a record of all categories of data that are provided or generated by business users and end users.[179]

However, the draft guidelines may impose **obligations that appear too demanding and without a particularly clear legal basis**.

- The suggestion that gatekeepers implement periodic reminders to end users about their personal data portability choices;[180]
- The suggestion that the gatekeeper make available tools to enable third parties to establish contact with individuals other than the end-user to help the personal data recipient comply with the GDPR;[181]
- The suggestion that gatekeepers should ensure appropriate visibility and accessibility of personal data portability solutions with dedicated interfaces.[182] One can see the rationale for this: presently all gatekeepers provide an option to port personal data, but this is not flagged clearly on the platforms, which may explain the relatively low take-up. On the other hand, we consider that other actors may be better positioned to inform users of the value of porting their data and making them aware of how they can do so or even providing services by which data can be ported easily.

These recommendations are significant contributions to the more general requirements of compliance in the DMA. They are based on Article 8 DMA which requires that gatekeepers demonstrate compliance and provide suggestions about how this may be achieved. It is worth recalling that Article 24 GDPR also requires that the controller 'shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.' In other words, **both Regulations require the design of compliant systems, with the DMA uniquely affording the opportunity for the Commission to receive reports on compliance**. These measures in the guidelines help regulated parties understand the expectations of the Commission and EDPB.

On the other hand, these are framed as suggestions (what a gatekeeper should do, not what it shall do) and it is not clear if they provide a safe harbour (i.e. if the gatekeeper follows, then there is a presumption of compliance, and if these measures are about securing compliance with the GDPR, the DMA, or both) nor if the refusal to follow these suggestions creates a risk of non-compliance. **The advantage of a more prescriptive approach, which should not go further than the obligations foreseen in the DMA and the GDPR, is that it provides greater certainty**, for example by suggesting

[177] Para 90.
[178] Para 111.
[179] Para 154.
[180] Para 123 and likewise for art 6(10) see para 164.
[181] Paras 114 and 116.
[182] Para 124.

that taking certain measures creates a safe harbour for compliance. It is also important that these recommendations have a **clear legal basis and that they are tested for proportionality**. There is nothing to stop the Commission from indicating measures that would be desirable, but if these are likely to be disproportionate then they can be flagged as optional steps without an obligation to apply them. Gatekeepers may have incentives to deploy these measures anyway if this can generate consumer demand.

2.3 The Digital Omnibus Package and the GDPR

As already indicated, in November 2025 the Commission presented a series of measures to amend some of the EU's digital laws to simplify the framework and improve competitiveness.[183] The proposals do not suggest amendments to the DMA, but some of the proposals to revise the GDPR have follow-on effects on the DMA, and we focus on this point here.

First, the **definition of personal data** is amended so that data is personal only if the controller can identify the individual "taking into account the means reasonably likely to be used by that entity."[184] This might facilitate the application of Article 6(11) DMA because it rests on a subjective interpretation of whether data is personal for the data controller.

Second, Article 9, which relates to **sensitive data** is amended so that an additional legal basis for processing this data is added: 'processing in the context of the development and operation of an AI system … or an AI model.' This may become relevant as the DMA might extend to regulate services that use AI technology.

3. Enforcement challenges

3.1. Public enforcement

3.1.1 Dialogue between regulators

The risk of multiple investigations into similar facts by different regulators has been discussed extensively. As we had suggested earlier, the ECJ case law has created a clear pathway to avoid the risk of decisions being quashed for failing to comply with the principle of ne bis in idem. A crucial component of this is **dialogue between all the national and the EU regulators (in charge of the protection of competition, the consumers, the privacy or the cybersecurity) involved in supervising the gatekeepers**, which is essential to avoid a finding that the rights of the gatekeeper have not been infringed.[185] Such dialogue seems to occur and the Commission is satisfied by the processes that are emerging, in particular with the competition authorities.[186]

[183] SWD(2025) 836 final. Article 3, amending Article 4 of the GDPR

[184] See here the Court's approach in Case C-413/23 P, EDPS v SRB, EU:C:2025:645, paras 68-89. Cf. EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) (10 February 2026), paras 16 and 17. Their criticism that the amendment goes beyond the judgment is unfair since the EU legislative body is entitled to modify secondary law. Moreover, it is arguable that the Commission proposal is in fact aligned with the judgment and merely clarifies a complex judgment, see especially the Courts insistence on limits to the notion of personal data at para 88.

[185] In this respect the joint guidelines para 216 are a bit oddly drafted as they seem to suggest that consultation is optional.

[186] Commission Second Annual DMA Report COM(2025) 166 final, paras 65-67.

Indeed, dialogue is particularly prominent with the Bundeskartellamt (BKA), given its **special competition powers** found in Section 19a GWB. The parallel application of such rule is foreseen in the DMA.[187] The German Federal Ministry for Economic Affairs and Energy has issued a report on the application of Section 19a and has noted that there has been close cooperation that in one case allowed the firm in question (Google) to "take a uniform approach to implementing the DMA obligations and the commitments made to the BKA."[188] The case in question extended Article 5(2) DMA obligations to other Google services not covered by the DMA.

Insofar as the BKA intervenes in markets not covered by the DMA (e.g., automobile infotainment systems) the law complements the DMA. However, it is possibly more problematic when the intervention addresses conduct by gatekeepers which extends the DMA obligations. For example, when Meta (whose Facebook service is a designated CPS) was forbidden under Section 19a to tie its VR glasses with Facebook, this is not conduct prohibited by Articles 5(7) or 5(8) of the DMA.[189] Indeed, some gatekeepers responses to the Commission DMA consultation point to the risk of fragmentation if NCAs apply their own rules on top of the DMA.[190] Fragmentation causes two kinds of negative effects: first, it makes compliance more costly because services have to be adapted for each Member State, insofar as the gatekeeper opts to only comply in one jurisdiction (e.g., in the VR Glasses case it appears Meta only offers a non-tied VR glass service in Germany).[191] And this has a second cost in that not all EU consumers gain from enforcement. On the other hand, when national authorities identify market failures that are not addressed by EU Law, this can stimulate better EU-level regulation.

Here, a **trade-off is made between an administrable legal system (one common set of rules) and a system with the potential to address missing market failures and allows regulatory experimentation (national differentiation)**. It is not clear to us that this trade-off has ever been discussed and it may be suboptimal to afford NCAs the option to always apply stricter measures. In this context, recall the Draghi Report's criticism of the gold-plating practices by Member States as one key factor harming competitiveness.[192] While he refers to the harm this causes to SMEs, there is follow-on harm also when large firms are subjected to different regulations. As the Facebook case shows, for example, an EU-wide remedy untying Facebook and VR equipment would be more likely to attract investment in VR devices that can interoperate with the services offered by tech giants.

Another example of this coordination may be found in the commitment decision issued by the Italian AGCM when applying **consumer law** to Google's consent model for the combined use of data (discussed also in 2.1 above). In this instance, the application of national law appears to overlap with the DMA. The AGCM coordinated enforcement with the Commission officials responsible for enforcing Article 5(2) DMA and also consulted with other national authorities (the regulator for electronic

[187] DMA, Recital 11 and Article 1(6).
[188] Bundesministerium fur Wirtschaft und Energie, Report pursuant to Section 19a (4) of the Act Against Restraints of Competition, page 6. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/E/20260107-evaluation-19a-gwb.pdf?__blob=publicationFile&v=6 Machine translation was used to read the text.
[189] J-U Franck, 'Abuse Proceedings Against Digital Gatekeepers under Section 19a of the German Competition Act: Taking Stock of Early Results (May 2024).
[190] European Commission, DMA Review - Summary of the contributions to the targeted consultation, call for evidence and AI consultation (2025), p.6.
[191] BKA, 'Meta (Facebook) responds to concerns of the Federal Cartel Office – VR glasses can also be used without a Facebook account in the future' 22 November 2022.
[192] The future of European competitiveness, Part A: A competitiveness strategy for Europe (2024) p.30.

communications (AGCOM) and the data protection authority).[193] It transpires from the documents that are publicly available that the Commission and Google also engaged in bilateral dialogue pertinent to resolving the issue in front of the Italian AGCM.[194] In its commitment decision, Google's actions are designed to comply both with consumer law and with the DMA. In this sense, while the Italian NCA is not directly competent to apply the DMA, it makes sense for the gatekeeper to achieve compliance with the DMA in parallel to avoid further proceedings. Unfortunately, it is not clear from the commitment decision whether the gatekeeper committed to this conduct for the EU as a whole, although it would appear that this is the case because one specific commitment (emailing end-users) was made specifically with respect to consumers based in Italy, suggesting the reminder of the commitments may be EU-wide.

There are two takeaways from these national decisions, which echo recommendations some of us have made already[195]. The best option in these settings **where a gatekeeper does not comply with EU Law (whether the DMA or other EU rules) would be for the Commission to apply the DMA and in the long term to consider the development of well-resourced EU-level digital enforcement agency**. This is particularly key in digital markets when the conduct of the firm is usually the same across jurisdictions. This ensures that a single approach is followed (ensuring legal certainty) and that the concerns are addressed across the whole EU market (ensuring effectiveness).

A good example in this context is the AGCM's investigation in Meta AI, where this conduct is now also considered by the Commission for all EU markets bar Italy.[196] The conduct under consideration is: (1) Meta integrating its Meta AI service with WhatsApp and (2) Meta doing the same in its WhatsApp Business Solutions, which is a service Meta offers to businesses for communicating with their customers. Here too, only Meta AI would be available as a chatbot or AI assistant. Interim measures were adopted by AGCM regarding the second practice because of the risk of lock-in: users will develop familiarity with Meta's chatbot and will be unlikely to switch to alternative services later in time.[197] Moreover, the use of Meta's chatbot will allow Meta to improve its services based on user queries, an option which would be denied to rivals who would then may enter with a less useful product for consumers.[198] These risks make interim measures necessary because, the AGCM reasoned, otherwise the market will no longer be contestable.[199] The Commission is now also considering the imposition of interim measures.[200] Two points are worth noting from these proceedings: first duplication is inefficient, and the Commission could take the initiative when there is a real problem at the EU level. Second, the agencies will necessarily have to coordinate a remedy, imposing added coordination costs that could easily be avoided. A further issue, which is beyond the scope of this paper, is the extent to which the conduct in question is also contrary to the DMA and not only EU competition law.[201]

[193] Case PS12714, Alphabet Inc and Google Ireland Ltd, Decision of 4 November 2025, Paras 11-13 https://agcm.it/dotcmsdoc/allegati-news/PS12714_acc.%20impegni%20+%20chius..pdf a press release in English is available at: https://en.agcm.it/en/media/press-releases/2025/11/PS12714.
[194] See https://www.agcm.it/dotcmsdoc/allegati-news/PS12714_testo%20impegni.pdf page 3.
[195] See Monti and de Streel, 'Improving EU Institutional Design to Better Supervise Digital Platforms' CERRE 2022.
[196] Commission opens antitrust investigation into Meta's new policy regarding AI providers' access to WhatsApp (4 December 2025).
[197] Case A576, Meta AI Chatbot (25 November 2025) Para 8 (https://www.agcm.it/dotcmsdoc/allegati-news/A576_provv.%20ampliam.%20istrutt.%20+%20avvio%20cautelare.pdf).
[198] Meta AI Chatbot, para 9.
[199] Meta AI Chatbot, para 12.
[200] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_310
[201] F. Bostoen and J. Kramer, "Is the DMA Ready for Agentic AI?" (CERRE 2025).

The second is that even if our first recommendation cannot be implemented in the short term, the **kind of coordination we see in these cases can allow for a reasonably resolution which does not jeopardise legal certainty and allows gatekeepers to comply in a manner consistent with all obligations**. One overarching idea that regulators should have in mind when coordinating enforcement is to ensure that this is as coherent as possible for the regulated firm. For example, if the firm has already complied with a DMA obligation in one manner and the national authority is extending the reach of that obligation to a new service, then the firm could simply extend its DMA compliance rather than being asked to devise another solution. The regulated firm should take an active role in this process of shaping and coordinating compliance. For example, if a data collection protocol that complies with art 5(2) is already in place and a national authority uses competition law or the GDPR to request additional limitations on the use of data in setting outside the DMA, then the firm should be able to replicate the protocols designed under the DMA.

3.1.2 Networks

Related to this, the case-law also requires institutional coordination when considering overlapping rules in order to avoid infringing the ne bis in idem principle. In this context, a proposal for a **Digital Clearing House 2.0** has been made by the European Data Protection Supervisor (EDPS) to enhance regulatory consistency and cooperation and facilitate the exchange of information.[202] On the one hand, this is desirable and there is evidence that cooperation among regulators is perceived to be useful in achieving these two objectives.

However, there may be **a risk of creating too many networks and duplicating resources**. For example, there are networks of national regulators in some Member States already and the DMA has its own High-Level Group which brings together expertise from a range of EU laws. The European Competition Network seems to be used to coordinate DMA related activity as well. Given that regulators are under-resourced, spreading individuals across too many networks may have an adverse effect on enforcement.

Such an initiative also requires a more fundamental reflection about how many EU and national agencies are needed to manage the digital rulebook. Rationalising this by reducing the number of agencies can also foster better internal dialogue about how to apply the rules. As suggested above, **centralised enforcement at EU level** can serve as a more effective way of integrating rules.[203] For example, if a single EU Digital Enforcement agency were in charge of DMA, competition and consumer law, one would have a series of internal processes to manage the links among these various laws.

Finally, it is inevitable that the EDPS would issue a recommendation which sees the GDPR, and the rights protected thereunder as the central point around which all other digital laws orbit. It is not clear that this is the most helpful premise for establishing a network of regulators. Conceptually, it is not clear that privacy and data protection rights should dominate other rights and interests. Rather, this project would be more effective if it were designed around two pillars: **(i) that trade-offs among various desirable policy objectives exist and must be addressed; (ii) that good regulation requires a learning environment by which the effects and side-effects of regulation should be considered**. This

[202] https://www.edps.europa.eu/data-protection/our-work/subjects/digital-clearinghouse-20_en.
[203] G. Monti and A. de Streel, Improving institutional design to better supervise digital platforms, CERRE Report, January 2022: Improving EU Institutional Design to Better Supervise Digital Platforms - CERRE.

means that the network would be well-placed to assess the extent to which regulation works and how to improve it. Such a pragmatic approach is preferable than staking out a principle about the normative superiority of data subject rights only to then undermine these rights given the exigencies of business models and the need to grow EU industry. Ultimately, regulatory consistency across legal instruments and across countries should reduce compliance costs and increase regulatory effectiveness.

3.2. Private enforcement

There has not yet been a large volume of private enforcement where the DMA is invoked. **Private enforcement may accelerate DMA enforcement** - especially because the Commission has limited capacity - and legal predictability in the long term as case-law and references to the ECJ can clarify the scope of the DMA.

At this stage we want to flag two issues that may require clarification and discussion. The first issue is how national courts should implement the duty of loyal coordination found in the *Masterfoods* judgment for antitrust cases and found in Article 39(5) of the DMA.[204] The key point is that a **national court should not issue decisions that contravene Commission decisions and stay proceedings pending a Commission decision**. Since a lot of compliance occurs via regulatory dialogue and sometimes solutions may occur even without the opening of proceedings, implementing this obligation can prove tricky. Courts should be able to secure information from the Commission about the state of play of any regulatory dialogue. Gatekeepers have a clear incentive to signal such dialogue to a national court.

The second issue pertains to injunctive relief. When claimants use the DMA to seek damages for non-compliance, there may be risks of a national court interpreting the DMA in a way that departs from the way the Commission would interpret the DMA. In this context, the usual pathway to clarify the law is using the preliminary ruling procedure. This is built into the way EU Law works and restated in Article 39(5) of the DMA. A slightly different issue may arise when it comes to **requests for injunctive relief, where a national court may be asked to impose a specific remedy on a gatekeeper, which could be compared to a Commission specification decision**.

In a recent judgment under the GDPR, the claimant had asked the national court to request an injunction 'prohibiting the controller from committing a further infringement of those rights.'[205] The ECJ found that there was no such right to an injunction on the basis of the GDPR. The question this gives rise to is whether under the DMA there is an EU-law right to such an injunction. On the one hand, the answer could be in the affirmative because the aim of the DMA is prospective: to open markets and to ensure that P2B relations are fair in the future. On the other hand, this entails two risks. The first is that the injunction imposes conduct which is too far-reaching in light of the DMA, and the second is that the gatekeeper is deprived of the option to decide how it wishes to comply with the DMA. Recall that when the Commission issues a non-compliance decision, it cannot stipulate how the gatekeeper shall comply[206]. Behavioural remedies may only be imposed when there has been systematic non-compliance[207]. Consequently, **given that public enforcement of the DMA sees**

[204] The judgment has been codified in Regulation 1/2003, Article 16.
[205] Case C-655/23, para 42, *IP v Quirin Privatbank AG*, EU:C:2025:655,
[206] Article 29(6) DMA.
[207] Article 18(1) DMA.

behavioural remedies as a last resort, there could be no EU law right to a forward-looking injunction on the basis of the DMA and when national courts have such powers, they should be exercised sparingly given that it is for gatekeepers to design compliance.

Having said that, **there may well be instances where there is only one route to compliance, and an injunction can prove effective**. A recent judgment in Germany for example compelled Google to allow end-users to use any email account they wish to sign up to set up an Android smartphone, basing its decision on Article 5(8) DMA. In this case, the gatekeeper has little option about how to design compliance.[208] An injunction on these facts is a proportionate remedy. However, there may be instances where affording gatekeepers the option to design compliance is preferable and an injunction may be framed in this manner rather than mandating specific conduct.

[208] https://dejure.org/dienste/vernetzung/rechtsprechung?Text=12%20HK%20O%2032/24 at the time of writing the judgment has not yet been published. A short summary is at: https://lawschoolgermany.de/blogs/zivilrecht/jura-online-nachhilfe.

About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network, digital industry, and service sectors. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.

About the Authors

Alexandre de Streel is the Academic Director of the digital research programme at CERRE, professor of European law at the University of Namur and visiting professor at the College of Europe (Bruges) and SciencesPo Paris. He sits in the scientific committees of the Knight-Georgetown Institute (US), the European University Institute-Centre for a Digital Society (Italy) and Mannheim Centre for Competition and Innovation (Germany). His main research areas are regulation and competition policy in the digital economy (telecommunications, platforms and data) as well as the legal issues raised by the developments of artificial intelligence. He regularly advises the European Union and international organisations on digital regulation.

Marc Bourreau is an Academic Co-Director at CERRE and Professor of Economics at Télécom Paris (Institut Polytechnique de Paris). He is affiliated with the interdisciplinary institute for innovation (i3) for his research.

His research focuses on competition policy and regulation, digital markets, and telecommunications.

Marc holds a Ph.D. in Economics from the University of Paris Panthéon Assas.

Richard Feasey is a CERRE Senior Adviser, an Inquiry Chair at the UK's Competition and Markets Authority and Member of the National Infrastructure Commission for Wales. He lectures at University College and Kings College London and the Judge Business School. He has previously been an adviser to the UK Payments Systems Regulator, the House of Lords EU Sub-Committee and to various international legal and economic advisory firms. He was Director of Public Policy for Vodafone plc between 2001 and 2013.

Jan Krämer is an Academic Co-Director at CERRE and a Professor at the University of Passau, Germany, where he holds the chair of Internet & Telecommunications Business.

He is editor and author of several interdisciplinary books on the regulation of telecommunications markets and has published numerous articles in the premier scholarly journals in Information Systems, Economics, Management and Marketing research on issues such as net neutrality, data and platform economy, and the design of electronic markets.

Professor Krämer has served as academic consultant for leading firms in the telecommunications and Internet industry, as well as for governmental institutions, such as the German Federal Ministry for Economic Affairs and the European Commission.

His current research focuses on the role of data for competition and innovation in online markets and the regulation of online platforms.

As the CERRE Director of Research, Zach Meyers has a wide remit, including managing our cross-sectoral programmes and projects.

Previously the assistant director of the Centre on European Reform, Zach Meyers has a recognised expertise in economic regulation and network industries such as telecoms, energy, payments, financial services and airports. In addition to advising in the private sector, with more than ten years' experience as a competition and regulatory lawyer, he has consulted to several governments, regulators and multilateral institutions on competition reforms in regulated sectors. He is also a regular contributor to media.

Zach holds a BA, LLB and a Master of Public & International Law from the University of Melbourne.

Giorgio Monti is a CERRE Research Fellow and Professor of Competition Law at Tilburg Law School. He began his career in the UK (Leicester 1993-2001 and London School of Economics (2001-2010) before taking up the Chair in competition law at the European University Institute in Florence, Italy (2010-2019). While at the EUI he helped establish the Florence Competition Program which carries out research and training for judges and executives. He also served as Head of the Law Department at the EUI. His principal field of research is competition law.

cerre

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank
CERRE Think Tank