cerre Centre on Regulation in Europe

INTERPLAY BETWEEN THE DMA AND OTHER REGULATIONS

GIORGIO MONTI
ALEXANDRE DE STREEL

cerre

Issue Paper

DMA Implementation Forum

Interplay Between the DMA and Other Regulations

Giorgio Monti
Alexandre de Streel

March 2025

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 report has been prepared, received the support and/or input of the following CERRE member organisations: ACM, Amazon, Apple, Arcep, Aspiegel, CnaM, Epic Games, Google, Media for Europe, Microsoft, Ofcom, and Qualcomm. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report 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

Table of Contents

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

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.

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.

1. Introduction

Over the past five years, the EU digital rulebook—along with its associated EU and national enforcers—has expanded significantly. As a result, the Digital Markets Act (DMA) is now just one of many laws that gatekeepers must comply with. It is, therefore, crucial that the DMA is enforced in a way that is consistent with the objectives and obligations of the other pieces of the digital rulebook. This will require close cooperation between the European Commission, which oversees the DMA, and the EU and national authorities responsible for enforcing the other parts of the digital rulebook. Achieving this may also necessitate a legislative effort to streamline the objectives and rules of the digital rulebook.

The purpose of this paper is to explore the regulatory interplay between the DMA and a selection of other key laws, specifically competition law, privacy law, and cybersecurity law. While other regulatory interactions—such as those with content law, consumer protection law, or intellectual property law—are also important, they will not be addressed in this paper. For each of the selected laws, this paper reviews regulatory overlaps, discusses issues that have arisen, and proposes ways to improve the overall effectiveness of regulation in this field. Additionally, we identify key uncertainties and interpretative questions and suggest possible approaches for addressing them.

2. The DMA and Competition Law

Generally speaking, EU and national competition laws continue to apply to firms that have been designated as gatekeepers.[1] But there are some limitations to the powers of National Competition Authorities (NCAs) and national courts.

This section focuses on the overlap between the DMA and the application of national and/or EU competition law by NCAs or national courts. We do not look at the possible overlaps that may arise between the DMA and the enforcement of EU competition law by the European Commission. We expect that this overlap is managed internally using the following criterion: **if the DMA applies, then the Commission will prefer applying it to EU competition law**. Not on the basis of a legal principle, but on the basis that the DMA has several institutional advantages that make it foreseeable that a quicker and more effective remedy may be obtained than under competition law.

Nothing prevents the Commission from **applying competition law to the conduct of a gatekeeper when its concerns are unrelated to obligations under the DMA**. Of course, there may be questions about whether a particular conduct is best characterised as circumvention of a DMA obligation rather than a stand-alone abuse of a dominant position and in this context different strategies might be considered.[2]

We leave it open whether there should be a priority rule in a revised version of the DMA. For example, a rule that requires the Commission to first examine if conduct may be better handled under competition law before proceeding under the DMA. It is not clear whether adding such a requirement would improve the regulatory process.[3] Moreover, given that the DMA seeks to promote different goals to competition law, it is not clear if such a priority rule makes sense. In electronic communications, the legislative intent was that regulation would eventually give way to competition law enforcement which made the priority rule logical in that economic context.

2.1 True Conflict between DMA and Competition Law

What happens if there is a conflict between compliance as required in the DMA and a remedy imposed on the basis of a breach of national competition law? According to Recital 10 of the DMA, the application of EU and national competition law 'should not affect the obligations imposed on gatekeepers under this Regulation and their uniform and effective application in the internal market.' This may be interpreted to mean that a **national competition authority cannot impose a remedy that would conflict with the gatekeeper's obligations**. This interpretation is followed by the Spanish competition authority in its Booking decision where it indicates that Booking may request a change to

[1] DMA, Article 1(6).

[2] For example, the Commission might prefer to start non-compliance proceedings and issue a decision to set a precedent about the scope of the concept of circumvention.

[3] G. Monti (2010) observes that UK regulators in the period 2000-2010 had to justify the application of sector specific regulation by showing that competition law would not be sufficient. The decisions surveyed showed that this requirement was treated in a perfunctory manner.

the remedies when there is a conflict with the firm's obligations under the DMA.[4] On this reading, the DMA prevails. Is this right?

An affirmative answer may be derived from the focus the DMA places on uniform application. A gatekeeper subject to a specific obligation under the DMA should not find itself bound by conflicting rules imposed by a national competition authority.[5] But **this only applies if there is a 'true conflict'** – that is to say the firm cannot possibly comply with two rules at the same time.[6] Consider the following examples:

a) Gatekeeper X implements procedures to comply with DMA Art 5(3) by making it clear to business users that they may henceforth set different prices when selling on ecommerce platforms other than the gatekeeper;

b) National Competition Authority 1 finds gatekeeper X to have abused its dominant position on an ecommerce platform and imposes a remedy that forbids the gatekeeper from ranking a business user higher if that business user sells via X's platform exclusively;

c) National court 2 finds that gatekeeper X has not abused its dominant position by giving ranking priority to business users who also use another of gatekeeper X's service.

There is no conflict between (a) and (b). The gatekeeper simply has more onerous obligations in the jurisdiction of NCA1. We do not discuss the extent to which the conduct in (b) is a circumvention of the DMA based on Article 13. The point is that there is no conflict between the obligations imposed by the Commission and the competition authority. All that happens is that the gatekeeper has additional obligations in the jurisdiction of NCA1. A scenario like this may be seen in the additional duties that Meta has in regard to data: it is bound both by the DMA and by the remedies agreed with the German Competition Authority.[7]

There is also no conflict between (a) and (c) because national court 2 does not require the firm to apply wide price parity clauses. Firm X can comply with both the DMA and competition law by complying with the stricter rule of the two. We use a court in this example because NCAs are not allowed to issue non-infringement decisions of EU competition law.[8]

The **only real conflict arises if the application of EU or national competition law by a national authority or national court would require that the gatekeeper behaves in a way that is forbidden by the DMA**. There is a remote chance of this scenario occurring because the two rules promote analogous objectives.[9] Moreover, if this were to arise the NCA would be in breach of EU Law and its

[4] Comisión nacional de los mercadoes y la competencia, Case S/0005/21, Booking (decision of 29 July 2024) Para 882 (https://www.cnmc.es/expedientes/s000521).
[5] A similar approach applies in EU competition law, see Case C-344/98, *Masterfoods Ltd v HB Ice Cream Ltd* EU:C:2000:689.
[6] J. Cremer, D. Dinielli, P. Heidhues, G. Kimmelman, G. Monti, R. Podszun, M. Schnitzer, F. Scott-Morton, A. de Streel, Enforcing the Digital Markets Act: Institutional Choices, Compliance, and Antitrust, *Journal of Antitrust Enforcement*, 2023.
[7] Bundeskartellamt, 'Facebook Proceeding Concluded' Press Release 10 October 2024. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/10_10_2024_Facebook.html
[8] Case C-375/09, *Prezes Urzędu Ochrony Konkurencji i Konsumentów v. Tele2 Polska sp. z o.o.* EU:C:2011:270.
[9] Hypothetically, if an Article 102 TFEU decision by the Commission were to require that a gatekeeper behave in a way that is contrary to the DMA, this decision would be lawful insofar as the Commission's application of primary law takes precedence over the Commission's application of secondary law but this scenario is unlikely to occur.

remedy unenforceable in the national courts because the NCA would require the gatekeeper to act contrary to EU Law.[10]

Therefore, **while it is correct to say that the DMA prevails over national competition law, the better view is that the conduct required of gatekeepers by the Commission under the DMA and remedies imposed by NCAs will hardly ever create a true conflict. Nevertheless, conflicts may arise as NCAs continue to exercise their enforcement powers. Moreover, a real challenge is ensuring that the two remedies are complementary**, which is discussed further below.

2.2 Competition Law and DMA as Multi-Layered Regulations

A criticism that has been made is that the DMA scores very poorly when it comes to harmonisation because it allows national competition authorities to add further remedies to gatekeepers which affects their planning and business models, and it places limited controls on Member States adding further legislation that overlaps with the DMA.[11] The only thing Member States are forbidden to do is to piggy back on the notion of gatekeeper as determined in the DMA and impose on these gatekeepers additional obligations. This is a very modest limitation. Thus, section 19a of the German Competition Act is in line with EU Law because, while its regulatory reach overlaps with that of the DMA, it has its own concept of 'paramount significance for competition across markets that has to be satisfied before obligations may be imposed. And even if some of the obligations overlap with the DMA, enforcement is still possible because these rules are applied on a different basis than that of the DMA. The concern is that it is too easy for Member States to supplement the DMA. Indeed, the application of section 19a by the Bundeskartellamt achieves outcomes where the same firms who are designated as gatekeepers find themselves with additional obligations that are at times an extension of what they are already obligated to do under the DMA.

It is difficult to bring a legal challenge against these laws. As explained above, they do not create a true conflict and there is no infringement of the *ne bis in idem* principle as often the facts are not identical. It is equally difficult to make a claim that a law such as the new Section 19a is contrary to EU Law since it is specifically authorised by the DMA. Member States have regularly insisted on 'gold-plating 'EU competition law. This was already evident during the debates that led to Regulation 1/2003; Member States agreed to the parallel application of EU and national competition law and with the provision that national law may not contradict EU law only if they were allowed to retain stricter national competition rules targeting unilateral conduct.[12] By this time, all Member States had reformed (or recently implemented) competition laws that replicated Articles 101 and 102 TFEU but some had retained some stricter norms which they wished to keep applying.

When the enforcement of EU competition law was decentralised, an **additional safeguard was built in by which once the Commission begins to consider certain conduct, then national competition authorities are no longer able to take action**.[13] In a similar setting, a national court applying EU

[10] Case C-198/01, *Consorzio Industrie Fiammiferi v Autoritá Garante della Concorrenza e del Mercato* EU:C:2003:430.
[11] https://cerre.eu/publications/better-law-making-and-evaluation-for-the-eu-digital-rulebook/.
[12] Regulation 1/2003, Article 3. For discussion see G. Monti *EC Competition Law* (2007) pp.406-409.
[13] Regulation 1/2003, Article 11(6).

competition law is also expected to stay proceedings pending a decision of the Commission.[14] After the Commission decides, then the national competition authority or national court may not reach decisions that conflict with that of the Commission. But this rule is only applicable when the national level institution (court or authority) applies EU competition law.[15] It would not apply if the national institution would rely on stricter national competition laws or apply any other rules of law that pursue different objectives. Therefore, this rule cannot be transplanted to the DMA context. One may argue that a similar priority rule could be built in by which the national laws cannot apply once the field has been covered by the DMA but then this cannot prevent a Member State from imposing additional obligations provided these are not contrary to EU Law.

Our view is that **what matters most of all is that there continues to exist dialogue between national authorities and the Commission when the former is looking to impose stricter requirements**. This appears to be occurring between the Commission and the German Competition Authority and has been commended by the European Parliament.[16] This is built into the DMA and it may be improved by setting out a procedure to structure this dialogue with firms. Presently what is governed is the exchange of information between the Commission and the NCAs and then only in specific moments. A more precise framework to structure coordination might help make coordination and compliance more effective.

NCAs could also develop a general principle that if the intervention of NCA2 or the Commission solves NCA1's concerns then the latter would not impose remedies. For example, if the Commission were to secure a change in compliance by the gatekeeper, then the NCA which remains competent would have to consider if continuing to pursue its competition law case is necessary or whether the Commission remedy removes the competition concern. This happens in merger control where remedies obtained in one jurisdiction may lead another competition authority to clear without adding further remedies.[17] This would avoid unnecessary duplication.

From an enforcement perspective, stricter requirements imposed on the basis of national law may be helpful in identifying additional market failures that are not covered by the DMA and which the legislator may not have foreseen. This allows for an improvement of the regulatory regime as these decisions may be used as a basis for revisions of the DMA. Franck for example takes the view that '[t]he 19a tool could thus permanently assume the role of a forerunner for possible regulation at EU level.[18]'

However, from another enforcement perspective, if the parallel application forces a gatekeeper to modify its conduct depending on the jurisdiction, this might be economically harmful: compliance costs may rise and a gatekeeper may be unwilling to offer its services in Member States where the behavioural remedies imposed are seen as excessively costly. It follows that just as the Commission should carry out an ex post impact analysis of the DMA, so should NCAs who have sector-specific

[14] Regulation 1/2003, Article 16 and see *Masterfoods* (above).
[15] If the Commission initiates proceedings in some Member States but excludes others, then the national competition authorities in the excluded States may apply competition law, see Case C-815/21 P *Amazon v Commission*, EU:C:2023:308.
[16] The EP 'encourages the Commission to pursue the coordination of enforcement activities and cooperate with national competition authorities in order to facilitate an effective interplay between competition law and the DMA, especially in the context of the DMA's 'further obligations' European Parliament resolution of 16 January 2024 on competition policy – annual report 2023 (2023/2077(INI)), para 39.
[17] 4a24a21a-en.pdf US submission.
[18] Page 51.

powers and it would be desirable if a commonly agreed method was found to assess the impact of regulation. One might go further and build on the concerns about over-regulation found in the Draghi report. In particular the report observes that one of the causes of the rising weight of EU regulation is that Member States 'gold plate 'EU legislation or 'implement laws with divergent requirements and standards from one country to another.[19]' While Draghi's concern was principally at the excessive burdens faced by SMEs, the same concern applies to gatekeepers: as shown above the example of the new German Laws gold plate the DMA. If this is unavoidable, then means to stimulate dialogue among regulators become ever more necessary.[20]

In sum, from a policy perspective, in the **short term**, there must continue to be dialogue among the Commission and regulators to ensure that enforcement actions are complementary. Perhaps, some mechanisms to contain extra regulation by national authorities would serve to clarify the regulatory burden: **an agreement that an NCA would not intervene unless the DMA does not address its competition concerns may be one mechanism that can be implemented without legislation**.

More **long-term**, the Commission may consider that **maximum harmonisation** is a better way of proceeding in regulating digital markets, thereby preventing the application of parallel national laws. It has moved in this direction in other fields.[21]

2.3 Two Principles to Manage the Legal Interactions

Having discussed some policy options for managing overlaps, we turn to the legal principles that apply.

2.3.1. Ne Bis in Idem Principle

First, **the principle of *ne bis in idem* governs the parallel application of the DMA and other laws. However, the scope of application and the degree of protection afforded by this principle is narrow**. The *ne bis in idem* principle means that a firm has the right not to be tried or punished twice for the same offence.[22] It requires a first punishment being meted out and this prevents a second investigation on the same facts. The commencement of a second investigation harms the reputation of the firm and imposes costs on it: this is the legal right that the principle protects.[23] A scenario where this right may be invoked is if there has been a non-compliance decision by the Commission under the DMA (which counts as a criminal procedure in light of the high penalties that may be imposed)[24] and then the start of competition proceedings by a national competition authority based on the same facts. In this context, the *ne bis in idem* principle applies because there has been a prior decision and a second proceeding begins which is directed against the same legal person based on the same,

[19] M. Draghi, *The Future of European Competitiveness – Part A* (September 2024), p.65.
[20] P. Larouche and A. de Streel, The integration of wide and narrow market investigations in EU economic law, in M. Motta, M. Peitz and H. Schweitzer (eds) *Market Investigations: A New Competition Tool for Europe?* Cambridge University Press, 2022, 164-215
[21] S. Weatherill, *Contract Law of the Internal Market* (2016) ch.6.
[22] Article 50, Charter of Fundamental Rights.
[23] B. Van Bockel, *The Ne Bis in Idem Principle in EU Law* (2010) pp.209-212.
[24] Case C-117/20, bpost v Autorité Belge de la concurrence EU:C:2021:689, paras 25-29.

identical, facts as the Commission decision.[25] Facts are identical having regard to the infringement period and the evidence under consideration.

However, the Court of Justice of the EU in *bpost* judgment held that a limitation of the right protected by *ne bis in idem* is allowed.[26] Generally, a second proceeding may be opened if this is necessary and it genuinely meets objectives of general interest recognized by the EU or the need to protect the rights and freedom of others.[27] The Court explained that this general principle may be analysed by considering a set of indicators. These are listed in table 1 on the left hand side and applied to the question of whether an NCA may apply competition law after the Commission has issued a non-compliance decision on the same facts.

Table 1: Ne bis in idem principle and the DMA

General principles of *ne bis in idem*	**Application when competition law is enforced after a final DMA decision is reached**
Second proceedings are provided by law	*Yes*: DMA, Art 1(5)
Two laws pursue distinct legitimate objectives	*Yes*: DMA aims at fairness and contestability, competition law at keeping markets open or consumer welfare
Proportionality: do we need the second proceeding to achieve the goals of competition law?	*Yes*, provided the accumulated legal response is not excessively burdensome for the firm.
Are there clear and precise rules to explain when there will be duplication and is there sufficient coordination between the authorities? Are the two proceedings sufficiently close in time? Is the overall fine excessive?	First question *Yes*: DMA, Arts 1(5) and 38. Second and third questions are a *matter of fact*

However, the **right protected by the principle of *ne bis in idem* is limited in two ways**:

- It only applies if the second enforcer in time considers the same facts. Thus, when the German NCA acts against a gatekeeper based on national law and considers exactly the same conduct as the Commission then the principle applies, but it does not apply if the NCA develops a different theory of harm that relies on additional evidence.

[25] Bpost (Ibid.), para 36.
[26] Based on Article 52 of the Charter of Fundamental Rights, which allows limitations on the exercise of rights and freedoms in certain circumstances.
[27] Bpost (Ibid.), para 41.

- It only applies if the first authority has initiated criminal proceedings. Decisions leading to a fine are normally treated as criminal because the high level of fines makes these sufficiently punitive. It is not clear however if a specification decision by the Commission triggers the right of protection under *ne bis in idem*, because specification decisions do not directly lead to a fine being imposed on the gatekeeper. A fine may be imposed only if there is no compliance with the specification decision, which requires the commencement of different proceedings.[28]

These two limitations mean that while *ne bis in idem* principle protects an important fundamental right, it is not a principle that may be invoked frequently in the DMA context. For example, the Spanish NCA decision on Booking's price parity clauses came before the DMA but penalised conduct that occurred in the past, while the DMA's obligation not to set price parity clauses applies prospectively from the date the DMA applies to booking. The *ne bis in idem* principle does not bite. However, as explained earlier, the Spanish NCA has built in a proviso that allows the firm to seek changes to the remedies should compliance with the DMA create problems with continued compliance with the Spanish decision. This opens the opportunity for reassessment but again the *ne bis in idem* principle is not applicable because the Spanish NCA considered a wider swath of conduct in its decision. The legal basis for this reconsideration is a more general principle of cooperation, which we now discuss.

2.3.2. Cooperation Principle

The example of the Booking decision reveals a second, more important, principle that should be the focus of attention: the **general legal duty of loyal cooperation (Article 4(3) TEU) requires that both Commission and NCA take care to coordinate their conduct**. And Article 38 DMA is designed precisely to achieve this. The duty to coordinate applies irrespectively of whether the same facts are being looked at and irrespective of whether the proceedings are criminal in nature. In practical terms, there are two key coordination moments in the DMA:

- When an NCA intends to start proceedings against a gatekeeper, it shall inform the Commission. Note that this information duty applies even if the Commission has taken no enforcement action against the gatekeeper and even if the action has no overlap with the DMA. The identity of the firm is all that matters for the duty to cooperate to start. This information may also be shared with other NCAs;
- A draft remedies decision shall also be sent to the Commission. Note that the Commission has no veto powers but the expectation is that this facilitates coordination to ensure that the remedy complements the DMA.

The NCA and Commission have the power to exchange information, including confidential information. The procedures in Article 38 ensure that there is compliance with the *ne bis in idem* principle but they also assist more generally in securing that there is good cooperation among NCAs when the same undertakings are being regulated. It creates a wider basis for ensuring that a consistent policy is pursued.

[28] DMA, Article 29(1)(c) and 30(1)(b).

NCAs who are members of the European Competition Network have experience with this and a soft law notice helps supplement Regulation 1/2003 to **ensure that the rights of the defence are protected**.[29] These are somewhat more extensive than under the DMA:[30]

- Information must be gathered lawfully according to the law applicable to the authority and the sending authority may inform the receiving authority if there is a legal challenge against the collection of this evidence. This is not provided for in the DMA, but in 2024 one is entitled to assume that NCAs and the Commission ensure the legality of searches. Matters were different in 2004 when Regulation 1/2003 came into force and many NCAs were just starting out. Moreover, the 2019 ECN+ Directive ensures harmonized procedures, including powers to inspect premises.[31] From this perspective, there is no need to prescribe this requirement under the DMA.
- Information covered by the obligation of professional secrecy is not to be disclosed. Under the DMA, Art 36 imposes this obligation on the Commission, but there is no corresponding provision on NCAs although one might expect this to be part of their protocols already. Again, one may legitimately expect that NCA officials will respect professional secrecy, not least since NCAs have this obligation under the ECN+ Directive.[32]
- On the basis of Regulation 1/2003, information coming from the Commission may only be used to apply national law when this does not lead to an outcome finding an infringement different from that under Arts 101 and 102 TFEU.[33] This means that if the Commission and the NCA are cooperating when both exercise their antitrust powers, then the NCA cannot use information received from the Commission to apply provisions like section 19a of the German Competition Law. This limitation is not found in the DMA: NCAs are free to apply any provision of national competition law. This is because Regulation 1/2003 foresees a scenario where both NCA and Commission are analysing the same case and a discussion is being had about which authority should be competent to take the case. Remember that the animating principle of Regulation 1/2003 is that each antitrust case should be addressed by one authority.[34] The purpose of the DMA is different and the Commission and NCAs are necessarily applying different rules so this safeguard is unnecessary.
- Information that is exchanged may not be used to impose sanctions on individuals save in specific circumstances. This is not found in the DMA. This omission is probably because the key concern of the DMA is to ensure that behavioural remedies are coordinated.

[29] Commission Notice on cooperation within the Network of Competition Authorities (Network Notice) [2004] OJ C 101/43.
[30] Network Notice paras 26-28.
[31] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (2019) OJ L11/3 (ECN+ Directive), Article 6 and more generally Article 3 confirming that national procedures shall comply with general principles of EU Law and the Charter of Fundamental Rights. The review of implementation suggests this has generally been transposed successfully. European Commission, Report on the transposition of Directive 2019/1 COM(2024) 558 final (29 November 2024).
[32] ECN+ Directive, Article 31(2).
[33] Regulation 1/2003 Article 12(2).
[34] One of us has repeatedly shown that this is a mistaken view because NCAs may only apply competition law to conduct occurring in or affecting its territory so that if a case having an effect on trade is assigned to one NCA this necessarily results in under-deterrence and remedies that do not solve competition concerns in the EU as a whole.

Article 38(1) DMA specifically foresees that implementing acts are necessary to ensure that arrangements for cooperation are based on a sound legal footing for NCAs who are not members of the European Competition Network. This will enhance the legitimacy of cooperation and safeguard fundamental rights. Cooperation is the most powerful mechanism to ensure that multiple enforcement actions are complementary and do not impose disproportionate requirements on gatekeepers.

The other gap in the DMA is that there is no provision explicitly coordinating fines when there are parallel infringements. Even if the *ne bis in idem* principle does not apply, it would be desirable to ensure that fines are coordinated to ensure that firms do not face disproportionate penalties. Fines should remain proportionate. The case-law on *ne bis in idem* allows for an ex post adjustment of fines: thus, the second authority imposing a fine must take into account the fine of the first authority. However, codifying this approach in soft law would be desirable.

3. The DMA and the GDPR

We have discussed the interplay between these two legal instruments in previous CERRE papers and do not propose to revisit that analysis there.[35]

3.1 Article 5(2) DMA

3.1.1. Consent or Pay Models

The main point of discussion in considering Article 5(2) DMA has been about how this is to be applied to gatekeepers whose business model is to combine use data from a variety of digital services when that data is used to sell advertising space. In this two-sided market, the consumer receives a service at no monetary fee in exchange for data and the business model is successful because this data can be exploited by the platform. There has always been a tension in the way this business model is utilised. On the one hand, some take the view that personal data is a right and that cannot be the basis of a market transaction. On the other hand, some take the view that data has economic value and that therefore a data subject should be entitled to relinquish its data rights in exchange for something else they value. Some brief reflections on this high-level point are in the box below.

The EU regulatory framework embraces two views about personal data that appear to clash. Generally, on the one hand, the GDPR safeguards user's rights to data. On the other hand, some EU legislation sees the economic value of that data, for example the data portability rules in the DMA. While some may argue that data portability confers on 'natural persons… control of their own personal data'[36] it is also the case that data portability is a means to engage in economic activities and obtaining better services.[37] At a conceptual level it is tricky to recognize the same object (data) as a human right protected for its own sake and as an asset which is valuable for the economic efficiency that results.

Looking at EU Law generally then, personal data has an economic value to both the person and the firms securing access to it. This however, clashes with the EDPB's view according to whom 'personal data cannot be considered as a tradeable commodity, and large online platforms should bear in mind the need of preventing the fundamental right to data protection from being transformed into a feature that data subjects have to pay to enjoy."[38] This statement is difficult to reconcile with the economic role that data plays. Striking an adequate balance between fundamental rights protection and economic utility is complex. Some have taken issue with whether consent as the basis for achieving this balance is satisfactory as data holders may not always be able to make good choices. Other ways of protecting fundamental rights have been suggested that would be more protective of data subjects. [39]

In this Issue Paper we do not question the importance of protecting the fundamental right to data, but we flag the tension in the legislative framework and raise a question about whether using consent

[35] G. Monti and A. de Streel 'Data-Related Obligations in the DMA' in A. de Streel (coord), *Implementing the DMA: Substantive and Procedural Principles* (CERRE 2024) pp.70-83.
[36] GDPR, Recital 7.
[37] See e.g. European Commission, Staff Working Document on Common European Data Spaces SWD(2024) 21 final.
[38] European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (17 April 2024), para 180.
[39] I. Cofone, *The Privacy Fallacy* (CUP, 2023).

as the mechanism by which data subjects can exercise their rights makes too many assumptions about the workability of this approach.

The consent or pay model has featured prominently in respect to the policies of one gatekeeper. At the time of writing, this gatekeeper announced a model which aligns with preferences of the Commission that we discussed in an earlier CERRE paper. In brief, end-users have a choice of three alternatives when accessing Facebook and Instagram: (i) a free version when they give consent to personal data being used by Meta; (ii) a free less-personalised version with less end-user data; (iii) a subscription version when even less data is collected in exchange for a monthly fee.[40] We do not examine the gatekeeper's compliance but want to draw attention to three general aspects that arise from the design of a consent or pay model.

First, as a matter of procedure what this episode reveals is the **importance of cooperation among the regulators when rules overlap**. This episode has seen the application of competition law and consumer law by national authorities, followed by the involvement of the European Data Protection Board and the Commission on the basis of the DMA. In September 2024, it was announced that the Commission and the EDPB would work jointly to provide further guidance on the application of the DMA and GDPR.[41] While this is a welcome development, it is not clear what the relationship is between this bilateral cooperation and the DMA High Level Group. Given that this also triggers competition and consumer law issues, it is not clear why bilateral dialogue is preferred. This raises a more general point about the role of the High Level Group.

Second, as a matter of substance it should be recalled that the **obligation in Article 5(2) is both procedural and substantive**. There must be an adequate choice architecture that allows the consumer to make a free, specific and informed choice and the choices must be compliant with Article 5(2).[42] Designing a good choice screen is a huge challenge because the less personalised version does require the end user to consent to some data and it is not clear how any choice screen can help a consumer understand the relative merits of the two free options. This goes back to our point in the box above that consent is a problematic benchmark in this context.

Third, this episode allows for a discussion about **what it means for a gatekeeper to offer 'less personalised but equivalent alternative**.' The comparison is between, on the one hand, the quality of the more personalized service (where the end user consents to data being shared for the provision of personalized ads) and, on the other hand, the less personalized service (where the end user does not consent to data being shared) offered by the same gatekeeper. It is not about what other service providers do. The quality of the two services may be assessed in two ways:

- One way is to compare the *functionalities* available to the end-user. These should be the same irrespective of the choice made;

[40] Facebook and Instagram to Offer Subscription for No Ads in Europe | Meta.
[41] https://digital-markets-act.ec.europa.eu/commission-services-and-edpb-will-start-joint-work-guidance-interplay-between-dma-and-gdpr-2024-09-10_en.
[42] Thus, a choice screen that tells the consumer 'for best results consent to sharing all your data' would probably not comply.

- A second comparator may be the *user experience* with the two different ways in which advertisements are provided. If the end user who opts for a less personalized services finds it hard to enjoy their navigation experience because of the volume of ads shown, this would suggest that the two services are not equivalent.

In this Issue Paper we take no view on what the right benchmark is but emphasise that this question is likely answered better via multi-disciplinary cooperation among regulators.

3.1.2 Article 5(2) DMA and Other Legal Contexts

It is important to bear in mind that Article 5(2) DMA is a rule that creates obligations between the gatekeeper and the end-user in order to achieve contestability.[43] The logic is to limit the amount of data gatekeepers can combine and reduce the advantages this gives them. From this perspective, it should be clear **that if the gatekeeper combines end-user data in ways that do not create barriers to contestability, then the obligation in the DMA should not apply**. For example, suppose a gatekeeper combines an end-user's data to work out if this end-user poses a risk to others, then the provisions of the GDPR apply but the DMA does not because this data collection policy has no impact on contestability. Conversely, the DMA does not forbid a gatekeeper from implementing measures to further protect the privacy of end-users, even going beyond what is required by the GDPR. Indeed, this is something that the DMA encourages by indicating that service providers should compete on privacy and data protection settings.[44]

This reading draws support from another data-related obligation, Article 6(2) DMA. Here the gatekeeper is allowed to obtain data but may not use that data for certain purposes. Protocols must be designed so that this data is only accessible to those who may use it for lawful purposes but may not be used by segments of the gatekeeper who could use that data to harm contestability in relevant markets. For example, a gatekeeper may collect data from business users and use this to improve its display functions, but may not use that data to develop goods or services that risk competing with those of the business users whose data it has access. But data may be used for these purposes lawfully only if such use is compatible with the GDPR.

If we generalise from these two points, we can conclude that the **data-related obligations in Article 5(2) apply to a gatekeeper to the extent that its business model reveals that the obligation is needed to ensure the objectives of the DMA are met**. In this context, it would be disproportionate to apply Article 5(2) DMA to conduct that does not have an effect on contestability.

The default rule is that gatekeepers are expected to comply with all the obligations set out in the DMA except for those that are reserved to a specific type of core platform service. However, in addition a gatekeeper may establish that a particular obligation does not apply, or applies only in part, if it can show that compliance would not have any effect on achieving the objectives of the DMA. **The burden of proof remains on the gatekeeper to explain why a particular obligation should not apply to it or should apply in a more limited form**.

[43] See also Recital 72 DMA: "The data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users."
[44] DMA, Recital 72.

The practical effect of this approach is that the gatekeeper would then only have to comply with the GDPR. This releases the gatekeeper from being only able to rely on consent as a means of being entitled to process personal data. The gatekeeper can then demonstrate that processing is necessary for the performance of a contact or necessary for the compliance of a legal obligation. The Court of Justice of the EU has read these restrictively; however it remains possible for a gatekeeper to avail itself of these legal bases if they can show that the data is not used to harm market contestability.

3.2 Data Portability

We have discussed this in earlier reports.[45] Generally speaking there is no overlap of rules in this context because the DMA provides a different routes to achieve legal portability. In brief, **Article 6(9) DMA appears to offer greater portability rights than the corresponding rules in the GDPR and the obligations on gatekeepers are also more extensive than those of data controllers in the GDPR**. The rationale is that the DMA imposes asymmetric regulation, placing a greater onus on the gatekeeper. It allows for data to be transferred when this would enhance contestability of markets by affording business users the chance to obtain as much data as possible to enter the market. As discussed above, it is clear that the DMA recognises the economic value of data and inserts requirements that are quite extensive and burdensome. Article 6(10) provides similar portability rights but this time for business users.

Table 2: Comparing GDPR and DMA on data portability[46]

	GDPR Art 20	DMA Art 6(9)	DMA Art 6(10)
Scope of data[47]	Data processed by automated means and personal data concerning the data subject	Data provided by the end user or generated through their activity on the CPS and 'any other data to effectively enable portability' (Rec 59)	Aggregated and non-aggregated data, incl. personal data provided or generated in the use of the CPS
Quality of access	Structured, commonly-used, machine-readable format.	in a usable format for end user and authorized third party (Rec 59)	Effective and high quality
Recipient	Right to transmit that data to another controller Where technically feasible, the data subject has the right to have the data transmitted directly to another controller	End users and third parties authorized by end users	Business user and third party authorized by the business user

[45] J. Kramer, 'Data Access provisions in the DMA' (CERRE, 2023).

[46] See also K. Bania and D. Katsifis, 'The Interplay between the DMA and Other Rules' in K. Bania and D. Geradin (eds), *The Digital Markets Act* (2024), pp.305-308. The main point the authors make is that the DMA does not complement the GDPR rights but does something different. We agree but do not consider this to be a problem per se, it only shows that recital 59 is badly drafted.

[47] For completeness, the data available is that which the data holder has obtained lawfully.

Tools		Gatekeeper shall provide tools to facilitate data portability (Rec 59)	Gatekeepers to provide appropriate technical measures, e.g. APIs or integrated tools for small volume business users (Rec 60)
Cost	Reasonable fee or refusal if requests are manifestly unfounded or excessive	Free of charge	Free of charge
Frequency		Continuous and real-time access	Continuous and real time
Limit	Right shall not adversely affect the rights and freedoms of others	None expressly provided but arguably the right shall not adversely affect the rights and freedoms of others.	with regard to personal data, access only if: (1) data is directly connected with services of business user; (2) end user opts in to sharing products or services
Safeguards	Controller may request information to confirm the identity of the data subject	None expressly provided, but: (i) as GDPR gatekeeper may confirm identity of data subject; (ii) compliance with other EU Laws may limit data transfers.	None expressly provided, but: (i) as GDPR gatekeeper may confirm identity of data subject; (ii) compliance with other EU Laws may limit data transfers.
Aim	Strengthen control of his or her data (Rec 68)	Contestability of CPS or innovation potential of the digital sector (Rec 59)	Contestability in a variety of industry sectors.

The table reveals just how asymmetric the regulatory framework is. The major difference when it comes to data portability for end-users is the requirement that data access is provided on a continuous and real-time basis. Another point of difference worth noting is that the GDPR builds some safeguards to allow the controller to verify the identity of the data subject, and similar safeguards may be implied in the DMA. Moreover, the GDPR also creates a procedure to govern the interaction between the data subject and controller. Conversely, the DMA expects that the gatekeeper will be responsible for designing a method of compliance that affords effective access to data. Can gatekeepers limit their obligations under these provisions?

One consideration relates to **the kind of data that is requested by the end user or business user**.

- The *maximalist view* is that the party requesting data has a right to request whatever data they wish for based on the DMA. This can be justified by the need to facilitate contestability and innovation and these processes require giving rival businesses as much information as possible to try and compete on the market. If some data turns out to be superfluous, this is irrelevant.

- A *minimalist view* is that the party requesting data should have a business model beforehand and present the gatekeeper with a request for specific types of data that are required to develop the business. This may be justified by invoking the principle of proportionality: the gatekeeper cannot be expected to incur costs to supply the data unless the business user shows that the data transfer is necessary to the new venture.

A balance between these two positions would be to afford the party requesting data the right to request what data they seek without requiring a detailed explanation of why they need it. A firm can motivate a request for data with a preliminary business plan. This is important to stimulate new entry and innovation.

Related, the requirement to provide continuous, real time data may not always be technically feasible. A gatekeeper should be able to demonstrate that there are limits to how this access can be provided such that it would be disproportionate to expect more from it.,

A final point is **whether the data access may be varied over time**. Suppose the initial portability requests is for data points A, B and C but later the recipient realises she only requires point A. At that moment, there should be an obligation on the recipient to vary the data request and a gatekeeper should be free to stop providing data B and C if it is clear that this is unnecessary. Otherwise, the gatekeeper incurs unnecessary costs of transferring useless data bundles. This argument is less valid for Article 6(9) where the end-user requests data and one should not question the end user's wishes.

Another consideration may relate to **the reputational risk that a gatekeeper incurs and the risk of data misuse that harms data subjects**.[48] This applies in particular when a third party receives data. This argument is a delicate one, however. First, while Article 6(4) DMA explicitly addresses the possibility of some vetting of third party providers, there is no mention of this in Articles 6(9) and (10). At the same time, when demonstrating compliance under Article 8(1) DMA the gatekeeper must reveal how it complies with EU Law more generally, which may require certain safeguards to protect users.

However, once data is transferred from gatekeeper to a third party, that third party becomes a data controller and as such has certain responsibilities vis-à-vis the data subject. Therefore, a gatekeeper should not use the risk of a third party infringing the GDPR as an excuse for not transferring data – self-help is not a remedy that the DMA appears to allow.[49] However, the end user may be unaware of the precise allocation of responsibilities and may well (unfairly) blame the gatekeeper for defective data management. To balance the rights of end users and business users on the one hand and gatekeepers on the other, a **gatekeeper should be allowed to warn users of the risks of porting data or to object to data transfers when the third party has been identified as not currently complying with GDPR by a national authority**.

Conversely, the reputational risk may be on the other side. Established firms are trusted by end-users who are thereby more likely to consent to requests to share data. Conversely a third party may be less trusted. This explains why Article 13(5) DMA requires that the gatekeeper shall 'take the necessary steps to … enable business users to directly obtain the required consent to their processing 'and 'shall not make the obtaining of that consent by the business user more burdensome than for its own

[48] Z. Meyers, *Which Governance Mechanisms for Open Tech Platforms?*, CERRE Report, January 2025.
[49] Likewise dominant firms may not take matters in their own hands to protect users, see Hilti v Commission.

services. 'In other words, the **DMA is less concerned with the reputational risk incurred by the gatekeeper than by the risk that the business user's capacity to secure consent from the end-user is hampered by the gatekeeper**.

4. The DMA and Cybersecurity rules

4.1 Openness and Cybersecurity

While several DMA obligations aim to open existing digital ecosystems in order to increase contestability, innovation and fairness, **such opening should not happen to the detriment of the security of the regulated core platforms services**. Safeguarding cybersecurity has become an increasingly important economic, societal and policy concern and objective in the Europe and in the world, particularly given the current evolution of international geo-politics. This is why the previous EU administration has adopted a series of new cybersecurity laws, in particular the revised Network and Information Systems Directive (NIS2) in 2022 and the Cyber Resilience Act (CRA) in 2024.[50]

The Cyber Resilience Act introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products. These obligations must be met at every stage of the value chain. Under the CRA, operating system and web browser providers are required to ensure baseline product security to manage risks across their platforms. In doing so, they need to take into consideration risks emanating from business users connected to their software, including through the access provisions of the DMA, such as alternative distribution and interoperability. While many business users of operating systems and browsers have also to manage risks related to interoperability, the scale of such risks for operating system providers is proportionate to the amount of business users they distribute or interoperate with.

At the outset, it is important to note that the **relationship between ecosystems' openness and cyber security is not unidirectional**.[51] On the one hand, more openness may improve resilience by increasing the numbers of providers of digital services as well as security by increasing competition on that dimension among those providers. On the other hand, more openness may also open new doors for hackers, cyberattacks and users manipulation undermining cybersecurity. Thus, ecosystems openness does not *per se* decrease security, but it should be organised in a way - in particular with governance mechanisms - which protects cybersecurity.

Moreover, the relationship between openness and cybersecurity depends on the competences and **cyber-literacy of the end users**. The literacy is particularly important as the digital ecosystems become more open and users are confronted with new choices, hence possible new security risks. Therefore, more users are competent, less the possible tension between openness and security will be.

This why gatekeepers should be able to develop users security empowerment tools like installation sheets, provided there are used in a transparent and non-discriminatory manner. In addition, Member States and national agencies may launch education campaigns as well as stimulated the establishment of independent security certification mechanisms.

[50] Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), OJ [2022] L 333/80 and Regulation 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations 168/2013 and 2019/1020 and Directive 2020/1828 (Cyber Resilience Act), *OJ L, 2024/2847, 20.11.2024*

[51] A. Bradford, The Optimal Size of a Tech Company, Draft, February 2025.

4.2 True Conflict and Trade-offs Between DMA and Cybersecurity

It is also important to note that digital platforms **and gatekeepers have private incentives to ensure the security of their ecosystem** in order to maintain the trust of their users; some platforms even use security as a competitive distinguishing factors against other providers. Platforms also have incentives to open their ecosystems to new app stores and apps developers in order to increase the value of their ecosystems.[52] But the optimal level of openness at the private level may not be the socially optimal one and this is why the DMA imposes more openness under some circumstances.

However, it is important that, in doing so, **the implementation of the DMA does not reduce the optimal level of security** and, crucially**,** it is key that the DMA does not impede the gatekeepers to comply with their obligations under the EU and national cybersecurity rules. Moreover, the implementation of the DMA should not reduce the **possibility of the platforms to differentiate** themselves and compete on security dimensions.[53]

To guarantee this, the DMA provides for specific **security and service integrity defences** (next to the privacy defences) attached to some of the DMA 'openness' obligations, in particular the obligations related to vertical and horizontal interoperability.[54] This defence allows the gatekeepers to take strictly necessary and proportionate measures to maintain the security and the integrity of their regulated digital services. In doing so, those defences allow a balancing between contestability and security and the consistency between DMA and EU cybersecurity laws in two different scenarios.

The first scenario is when there is a *true conflict* between the DMA and EU or national cybersecurity laws as understood in the section 2 i.e. that a gatekeeper cannot possibly comply with two rules at the same time. In this scenario, the **DMA security defence allows a gatekeeper to take the measures imposed by EU cybersecurity rules** and ensure that the DMA does not impinge on the ability of the gatekeepers to comply with their obligations under the EU and national cybersecurity laws. Moreover, if different measures comply with cybersecurity rules and achieve the same degree of security, the principle of proportionality implies that the gatekeeper should choose the one which is the least detrimental to contestability and fairness.

The second scenario is when there is no true to conflict between the DMA and cybersecurity rules but a gatekeeper wants to impose additional security measures than those imposed under EU laws. In this scenario, the application of the principle of proportionality of the security defence would require a **weighing the impact on cybersecurity against the benefits of contestability and fairness** where there is a trade-off.[55]

[52] M.G. Jacobides, Cennamo C., Gawer A. 2024. Externalities and complementarities in platforms and ecosystems: From structural solutions to endogenous failures. *Research Policy*, vol. 53

[53] M. Bauer and D. Pandya, Cybersecurity at Risk: How the EU's Digital Markets Act Could Undermine Security across Mobile Operating Systems, ECIPE Policy Brief 04/2025.

[54] DMA, Art. 6(3), 6(4), 6(7), 7(3) and 7(6).

[55] Z. Meyers, Balancing security and contestability in the DMA: the case of app stores, European Competition Journal, 2024.

4.3 Process and Governance Mechanisms to Manage Legal Interactions

Thus for both scenarios, the application of the integrity and security defences – and more generally the optimal balance between openness and security *when* they are in tension – may be difficult to apply in practice because it involves, on the one hand, complex technical questions[56] and, on the other hand, novel legal interpretations issues regarding the DMA (such are the exact scope of the security defence) as well as the EU cybersecurity laws (such as the exact security measures to be taken by the providers of operating system and web browser). Those difficulties require robust process and governance mechanisms to deal with the interactions between the DMA and cybersecurity laws.

First, the Commission should closely **cooperate with EU and national cybersecurity agencies** – in particular ENISA- to guarantee a consistent application of the DMA and cybersecurity rules. On the medium term, the composition of the DMA High Level group could be expanded to cybersecurity agencies. It is also important that the Commission build internal expertise and could rely on best external expertise in cybersecurity matters.[57]

Second, the Commission could clarify through **specification decisions and/or guidelines** how the scope and the application security and integrity defence will be interpreted by the Commission.[58]

Third, the Commission should incentivise the gatekeepers and the business users to agree on **inclusive governance mechanisms**[59] which could reduce the possible tension between contestability and security and guarantee that level of cybersecurity is not compromised by the increased openness of a digital ecosystem.

Those governance mechanisms could include:

- The continuous development of security **standard**s;
- Independent third-party or gatekeeper non-discriminatory automated **certification mechanisms** to ensure that the app stores and app developers having access to the open digital ecosystems are sufficiently secure;
- Independent and rapid **dispute resolution mechanisms** when there is a disagreement between the gatekeepers and business users on the implementation of the security defence.[60] In this regard, the establishment of an independent conciliation process that the Commission proposes in its draft specification decision on the process of interoperability applicable to Apple may a be step in the right direction.[61]

[56] Landis, Bietti, Park, SoK: "Interoperability vs Security" Arguments: A Technical Framework, 2025.
[57] Including through studies as currently done: https://digital-markets-act.ec.europa.eu/dma-commission-launches-call-tenders-study-mobile-ecosystems-2023-09-19_en; a study looking at specific security concerns that could arise in relation to i) uninstallation, ii) alternative app distribution , and iii) alternative browser engines.
[58] Z. Meyers, fn 55.
[59] https://cerre.eu/publications/which-governance-mechanisms-for-open-tech-platforms/
[60] Z. Meyers, fn 55 referring to the dispute resolution mechanisms which have been established in telecommunications regulation.
[61] Draft Decision, paras 43-47 : https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100204

5. Gatekeepers in Other EU Laws

In this section, we consider two developments – the choice to exclude gatekeepers from the benefit of EU Laws (5.1) and the extension of gatekeeper obligations in other laws (5.2). We present and discuss two specific policy initiatives below. At a more general level, these developments need further justification and analysis. The notion of gatekeeper was developed specifically to address concerns about contestability and fairness in a given set of core platform services. **It is not obvious that this notion is also useful in contexts outside the DMA, which is a Regulation that addresses a set of specific markets**. At most, there should be an ex ante analysis about whether the concept of gatekeeper is fit for purpose in other domains. Otherwise there is a risk that regulation is not addressed to the right actors. It may well be that asymmetric regulation is required under other EU Laws, but then selecting the target for higher regulatory requirement must be based on the ordinary regulatory impact assessment, and not a mechanical transposition of the gatekeeper concept.

5.1 Excluding Gatekeepers from the Benefits of EU Laws

In some regulatory frameworks that have come in after the DMA, the EU has elected to exclude gatekeepers from the benefits of new regulation. The **Data Act** explicitly excludes gatekeepers as defined and designated in the DMA from being able to obtain data: they can neither obtain nor solicit such data.[62]

> *Article 5(3)*
>
> *Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925, shall not be an eligible third party under this Article and therefore shall not:*
>
> *(a) solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services that the user has obtained pursuant to a request under Article 4(1);*
>
> *(b) solicit or commercially incentivise a user to request the data holder to make data available to one of its services pursuant to paragraph 1 of this Article;*
>
> *(c) receive data from a user that the user has obtained pursuant to a request under Article 4(1).*

This is explained in Recital 40 which states that the aim of the legislation is to benefit start-ups and small firms as well as forms from traditional sectors which have 'less developed digital capabilities.'[63] In contrast, gatekeepers already have 'unrivalled ability' to acquire data and it is seen as disproportionate to give them access to more data. The 'fairness of the distribution of data value across market actors' would otherwise be hampered. However, this merely prevents the consumer

[62] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L,2023/2854 (22/12/2023), Article 5(3).
[63] Data Act, Recital 40.

from requesting that data held by another firm is shared with a gatekeeper. Recital 40 closes by stating that "As voluntary agreements between gatekeepers and data holders remain unaffected, the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services." This means that there can be certain datasets that can be transferred lawfully to gatekeepers.

The criticism that may be made of this approach is that it **seems to deny the consumer's rights as co-creator of data**. The data in question is generated when the consumer uses the goods or services of a firm. In this context, the Data Act empowers the consumer to demand that 'his/her' data is shared with another service provider and it is not clear why it is not proportionate to allow them to share this data with a gatekeeper who may be able to cover precisely the service that the consumer wants and for which the consumer's data is an essential input. It is true that some gatekeepers already have a huge trove of data which confers on them competitive advantages, but this concern is not addressed by stifling the development of valuable services which some gatekeepers may be best placed to provide. Moreover, the DMA already contains data-related obligations designed to address this source of economic power in specific contexts.

This is an unfortunate development. The DMA does not prevent a gatekeeper from benefiting from the obligations that are imposed upon other gatekeepers. In markets like internet search or app stores, the **quickest way to create contestability would seem to be to facilitate market access to existing actors some of whom may well be gatekeepers in other core platform services**. Gatekeepers also have less fear of retaliation and may thus be key to forcing changes on rival gatekeepers that can then benefit all other business users. Nor does the DMA have specific rules to prevent the growth of a firm offering core platform services.

In sum, it is not shown that by excluding gatekeepers from the Data Act one enhances the objectives of the Data Act itself, which is about facilitating entry of market players who can make use of data to provide innovative services. It seems like the Data Act exclusion is designed to achieve, indirectly, the aims of the DMA.

5.2 Extending Gatekeeper Obligations in Other EU Laws

It may also be tempting to extend the regulation of gatekeepers in other regulations. For example, in reforming the **EU Merger Regulation's** jurisdictional thresholds one could provide that all acquisitions by a gatekeeper must be notified. And its call for evidence on virtual worlds the Commission uses the notion of gatekeeper.[64]

In financial services, the European Banking Authority (EBA) has observed that some gatekeepers have entered certain financial sectors – especially e-money and payment services, even if so far entry is modest. The EBA study considers the entry of a wider range of tech firms too.[65] The study reports that

[64] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13757-Virtual-worlds-metaverses-a-vision-for-openness-safety-and-respect_en

[65] Amazon, Alibaba (Ant Group), Apple, Baidu (Du Xiaoman), Google, JD.com, Mercado Libre, Meta Platforms (previously Facebook), Microsoft, NTT Docomo, Rakuten, Samsung, Tencent, Tesla, Uber, Vodafone and Orange. https://www.eiopa.europa.eu/document/download/3fccfa9e-7dbf-49ce-afa9-

firms like gatekeepers are well placed to participate in the provision of financial services but that they also create certain risks because of their wider portfolio of services. A plausible regulatory response could be that the gatekeeper notion is extended to financial market regulation so that gatekeepers are placed under scrutiny by financial service authorities. It is not clear if the gatekeeper label however is sufficiently capacious to include all tech firms that may create financial risks. As suggested above, our preference is to base any asymmetric regulation on an impact assessment that identifies the right target for such regulation.

In the proposed **Regulation on Financial Data Access (FiDA), gatekeepers are given special attention**.[66] The Regulation aims to facilitate access and sharing of customer data in financial services to stimulate the provision of innovative services including personalized financial products. FiDA is expected to reduce entry barriers by facilitating switching by creating a harmonized framework for access to financial data.[67] The text is currently under negotiation and the current version may be used to explain and discuss the kinds of regulatory choices that are envisaged when it comes to gatekeepers.

Originally, the European Parliament had suggested excluding gatekeepers altogether, like in the Data Act. The current draft under discussion however, allows gatekeepers to benefit from the Regulation with certain limitations.

First, Draft FiDA Article 6(4b) indicates that the gatekeeper cannot combine the data it obtains under this Regulation with other data that it has.[68] This is stricter than DMA Art 5(2) because combination is not allowed even if the consumer were to consent. This requires specific justification that explains what risk this seeks to combat and why this risk manifests only when gatekeepers act in this way and no other actors.

Second, Draft FiDA Article 12 provides that a financial information service provider wishes to access customer data must be authorized by the competent authority of the Member State of establishment. Article 12(4a) provides that when such an application comes from a gatekeeper then a specific assessment is performed which is also considered by the ESA. The special assessment regime is provided for in Draft Article 18a.

Focusing on the substance, the competent authority should consider the following:

(a) a programme of operations submitted by the gatekeeper setting out the functioning, services and activities performed, access to customer data and the size of activity.

(b) Network effects and data driven advantages of the gatekeeper 'in particular in relation to that undertaking's access to, and collection of, customer data or analytics capabilities'

8abfa22df22a_en?filename=Joint%20ESAs%20Report%20-%20Stocktaking%20of%20BigTech%20direct%20financial%20services%20provision%20in%202023.pdf.

[66] The current draft is available at: https://data.consilium.europa.eu/doc/document/ST-16312-2024-INIT/en/pdf (published on 2 December 2024).

[67] Useful background may be found at: https://www.financial-data-access.com/.

[68] FiDA Art 6(4)(f): "Data users that are designated as a gatekeeper or that are owned or controlled by an undertaking that has been designated as a gatekeeper shall be prohibited from combining customer data referred to in Article 2(1) of this Regulation with other data relating to the customer that the designated gatekeeper may already collect, store, or otherwise possess for purposes outside this Regulation."

(c) Evidence that the entity has in place sufficient safeguards to demonstrate compliance with Articles 5 – 8 of the Regulation

(d) 'evidence that the entity 'has in place sufficient IT, governance and organizational safeguards to demonstrate compliance with Article 6(4)(f),[69] and that the segregation of data is ensured at all times and permanently in accordance with Article 6(4b)'

Items (a) and (b) are supplementary checks: only gatekeepers that satisfy these two requirements fall under FiDA. However, some guidance on how to decide when the economic criteria in (b) are met would be helpful. On the one hand, one might see this as a useful way of avoiding over-regulation because not all gatekeepers will this be subject to this regime. On the other hand, the very fact that the concept of gatekeeper is not sufficient to identify the target of asymmetric regulation suggests that transplanting the gatekeeper concept here is not satisfactory as a way to regulate markets.

The substantive risk-assessment is carried out under items (c) and (d) by which the competent authority ensures that there is no risk that the gatekeeper can leverage its competitive advantages.[70] This means that gatekeepers can participate in these markets provided that they do not combine the data in order to achieve a competitive advantage over other entrants. At a micro-level, this requires some additional specification to identify the degree of network effects and data driven advantages that are sufficiently high to warrant closer supervision to ensure that intervention is proportionate. However, more generally, it is not clear why these additional requirements are necessary before allowing the entry of gatekeepers.

Generally, FiDA proposes a stricter regime for gatekeepers both in regulating their entry into the market and then controlling their conduct. There are two general concerns about this approach. First, as indicated above, without an ex ante impact assessment that identifies market failures that need to be addressed then the proposal is not well-justified. Second, some of the strictness of FiDA for gatekeepers seems to be designed to address contestability concerns which are part of the DMA, while FiDA is legislation has other objectives. It is designed to empower customers of financial institutions and to stimulate the development of innovative financial products and services.[71] We suggest further reflection is needed before inserting additional requirements for DMA-designated gatekeepers in other elements of EU regulation that are designed for different reasons.

[69] This provides that 'where the data user is part of a group of companies, customer data listed in Article 2(1) shall only be accessed and processed by the entity of the group that acts as a data user.'

[70] FiDA Draft Regulation, Articles 18(5) and (6) provides that the gatekeeper may modify its plans f they are deemed unsatisfactory.

[71] FiDA Draft Regulation, Recitals 1 and 3.

cerre Centre on Regulation in Europe

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