cerre

OPEN TECH PLATFORMS: TECHNOLOGY AND GOVERNANCE MECHANISMS

ISSUE PAPER

February 2026

Zach Meyers

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, DuckDuckGo, EETT, Google, Mozilla, 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

Executive Summary

EU policymakers increasingly view platform "openness" as a central tool for strengthening competition, resilience and innovation in digital markets. The Digital Markets Act (DMA) gives legal effect to this ambition by mandating greater data portability and interoperability for certain platforms operated by gatekeepers.

This paper does not examine the economic case for mandating greater openness under the DMA. Instead, it focuses on a more practical question: given the DMA's rules do mandate more openness, how can those obligations be implemented in a way that is effective, proportionate, and consistent with privacy, security, and innovation incentives?

While the DMA sets out high-level 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. The 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.

Table of Contents

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.[1]

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

- Rules on '**data portability**' can help end-users[2] and business users[3] 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;[4]
- Rules on '**horizontal interoperability**'[5] aim to allow providers of online communications services like instant messaging[6] 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**'[7] 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

[1] 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.
[2] Art 6(9).
[3] Art 6(10).
[4] Jan Krämer, Pierre Senellart and Alexandre de Streel, 'Making data portability more effective for the digital economy', CERRE Report, 2020.
[5] Art 7.
[6] Known in the DMA as 'number-independent interpersonal communications services' or NIICS.
[7] 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.

not always[8] – 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.

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-

[8] Carmelo Cennamo and Zach Meyers, 'Mandating Openness in Regulated Markets', CERRE, forthcoming.

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"[9];
- 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.[10]

The GDPR already provides a right for users to port their data in a "structured, commonly used and machine-readable format".[11] 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.[12] 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.[13] The purpose is so that a

[9] DMA art 6(9).
[10] DMA art 6(10).
[11] GDPR art 20; see https://cerre.eu/publications/effective-and-proportionate-implementation-of-the-dma-3/.
[12] Under the GDPR, service-to-service transfers only need to be provided where "technically feasible".
[13] 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.[14] 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.[15] 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.

[14] DMA art 6(7).
[15] 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**)[16] 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

[16] 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;[17]
- 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.[18]

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".[19] 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,

[17] https://dtinit.org/.
[18] Zach Meyers, 'Which Governance Mechanisms for Open Tech Platforms?', CERRE, January 2025.
[19] 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:**[20]

- 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

[20] 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.[21]

In the Draft Guidelines, there is a recognition that gatekeepers have a legitimate need to onboard third party recipients of data[22] and ensure "authentication procedures (including to verify the authorisation granted by end users to a requesting third party)".[23] 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".[24] 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".[25]

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.

[21] Data Transfer Initiative, 'A third-party trust model for direct personal data transfers'.
[22] Para 130.
[23] Para 132.
[24] Para 113.
[25] Draft Guidelines, para 131.

Furthermore, the DMA's interoperability rules – which have similar potential for privacy and security 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. [26]

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,

[26] 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.

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 fail to comply risking having their regulatory permissions revoked.[27] 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".[28] 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).[29]

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

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

costs – that is, whether more costs should be borne by gatekeepers or by firms trying to take 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.[30] It envisages that the Commission can request European standardisation bodies to develop appropriate standards.[31] 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,[32] 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.[33] 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.

[30] DMA recital 96.
[31] DMA art 48.
[32] https://mas.owasp.org/.
[33] Chris Riley and James Vasile, 'Interoperability as a Lens onto Regulatory Paradigms', CPI, 2021.

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 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.[34] CODE also has (as noted above) an 'Ethical Data Badge' initiative which also verifies accredited firms as being trustworthy recipients of data.[35] 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.

[34] Data Transfer Initiative, 'Update on trust efforts at DTI', 30 July 2024.
[35] 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.[36] 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"[37] 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

[36] BEUC, 'First Bloom: Increased Consumer Choice after Eighteen Months of the DMA', November 2025, p 9.
[37] 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.[38]

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

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

the specification tool to mandate that gatekeepers adopt more consistency in the design 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.[39]

[39] 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.[40] 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.[41] 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.

[40] 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.
[41] 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.[42] 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.[43] 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

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

particular business user is a legitimate recipient of data or access to system functionality. As noted above, the Data Transfer Initiative's Trust Registry – which sets out which firms are safe recipients of ported data[44] 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.[45] 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

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

among many stakeholders that public workshops may not be the most effective way of driving 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)[46] 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**.[47] 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.

[46] https://dtinit.org/.
[47] 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.

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 Author

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.

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