cerre Centre on Regulation in Europe

DATA-RELATED OBLIGATIONS IN THE DMA

GIORGIO MONTI
ALEXANDRE DE STREEL

January 2024

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: Amazon, Apple, Booking.com, DuckDuckGo, Epic Games, Google, Aspiegel, MFE-MediaForEurope, Meta, Microsoft, Mozilla Corporation, 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 top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

1. its original, multidisciplinary and cross-sector approach;
2. the widely acknowledged academic credentials and policy experience of its team and associated staff members;
3. its scientific independence and impartiality;
4. the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their 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 at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

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.

Alexandre de Streel is the Academic Director of the digital research programme at CERRE and Professor of European law at the University of Namur where he chairs the Namur Digital Institute (NADI). Alexandre is also visiting professor at the College of Europe (Bruges) and SciencesPo Paris. Besides, he chairs the expert group on the online platform economy advising the European Commission and is a part-time judge at the Belgian Competition Authority. His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence.

Previously, Alexandre held visiting positions at New York University Law School, European University Institute in Florence, Barcelona Graduate School of Economics and University of Louvain. He also worked for the Belgian Deputy Prime Minister, the Belgian Permanent Representation to the European Union and the European Commission.

FOREWORD

In the dynamic landscape of EU digital platforms regulation, we are at a focal point of discussions shaping the future of implementation of the Digital Markets Act – arguably one of the most important pieces of legislation of the current times' digital policy sphere.

With the DMA aiming for contestability and fairness in digital markets, designated gatekeeper platforms are set to unveil their compliance plans on March 2024. The European Commission, in its unique role as an enforcer, will lead the work of determining non-compliance and ensure that the DMA fulfils its ambitious goals.

However, the success of implementation will depend on the principles on which the new law will be applied. This CERRE report recommends that the DMA implementation process should be guided by the substantive principles of effectiveness, proportionality, non-discrimination, legal predictability, and consistency with other EU laws. Furthermore, the Commission will have to approach enforcement taking into account the procedural principles of responsive regulation and participation, due process, and ex ante and ex post evaluation. The report then applies those principles to series of specific DMA obligations: choice architecture, horizontal and vertical interoperability and data related obligations.

It is also essential to agree on how the Commission, gatekeepers, and third parties will engage with each other. The DMA provides a model of compliance which is not based solely on deterrence; instead, the gatekeepers are encouraged to and will comply by engaging co-operatively with the Commission and third parties. However, it is still up for question how this principle will be applied, what it expects from the stakeholders, and how the Commission itself will exercise its deterring powers to enforce compliance.

On top of it all, this CERRE DMA edition is also proposing a set of quantitative measurement indicators, so-called output indicators, each relating to a particular obligation or set of obligations, in order to better understand the impact of obligations on the relations between gatekeepers and third parties. These quantitative indicators will not represent specific targets or thresholds against which compliance should be assessed. They will neither attempt to measure the effect of changes in conduct on market outcomes for users nor, more generally, competition. These quantitative measures will be added to other evidence, such as complaints or qualitative representations from affected parties, including gatekeepers, which the Commission will consider in its compliance assessments.

This report was written in the framework of a 8-month-long, multi-stakeholder CERRE initiative entitled the 'DMA Compliance Forum' that created a neutral and trusted platform and facilitated dialogue among CERRE members and academics to contribute to the effective and proportionate enforcement of the regulation.

Bruno Liebhaberg, CERRE Director General

1. INTRODUCTION

In this paper we discuss the four data-related obligations in the DMA. Each of the four rules is discussed using the following structure: (1) purpose and content of the rule, (2) principles for implementation and (3) relationship with other rules.

Identifying the purpose of these provisions and how that purpose is translated in the legal text matters because it allows us to see how far the rules are capable of supporting the objectives set and because EU law is interpreted having regard to the purpose of the rules. Our view is that **the data-related obligations predominantly pursue the aim of contestability. In this context, it is worth noting that in making markets more contestable attention is paid to dynamic competition**. A useful distinction in this respect is between sustaining and disruptive innovation. Sustaining innovation occurs when a firm creates a better performing service (e.g., a taxi company improves its online booking system), while disruptive innovation creates new markets (e.g. Uber). The DMA should support both.

The discussion then moves to how these rules may be complied with. Here we suggest that two legal principles matter: (i) effectiveness; (ii) proportionality:

- Every rule aspires to be **effective,** but the DMA is particularly focused on ensuring that gatekeepers comply in a manner that achieves some change in the market – it follows that the Commission will look closely at the design of compliance and will ask for a reflexive approach by gatekeepers by which they revisit their compliance methods regularly. How this is achieved is the subject of the companion paper on DMA process and compliance. At the same time, effective compliance should not lead to gatekeepers implementing solutions that do not reflect consumer preferences.

- **Proportionality** means that the gatekeeper is expected to implement the obligations in a way that is effective but not disproportionate in achieving the objectives of the DMA. This balances the business freedom of the gatekeeper with the interests of opening up markets. More specifically, if there are two, equally effective ways of complying, then the gatekeeper may take the least onerous way.

There is a possible tension between proportionality and effectiveness because a regulator has a preference for the most effective method of compliance, but the gatekeeper is not bound to maximise the effectiveness of the DMA, only to comply with the rules. The gatekeeper does not have a 'special responsibility' to make markets work better.[1]

In the third segment of each part, we discuss the relationship between the DMA obligation under discussion and other DMA rules as well as other rules of EU Law, especially the General Data Protection Regulation (GDPR).

[1] As is well-known the ECJ has held that a dominant undertaking has a special responsibility but even there it is a responsibility not to harm competition, not a responsibility to make markets more competitive.

2. ARTICLE 5(2) DMA

2.1. Purpose and Interpretation

2.1.1. Purpose

It is important to recall that Article 5(2) does **not prohibit the continuation of a business model based on data collection** by gatekeepers. While this model has been the subject of criticism, the DMA simply places limits on data collection by requiring explicit consent on the part of the user. The primary purpose of this limit is to make markets more contestable.[2] **Contestability is expected to manifest itself in three markets**.

First, limiting the data collection capacity of gatekeepers means that rival providers of core platform services have a more level playing field. Presently the concern is that the gatekeeper gains advantages by accumulating data and this raises entry barriers.[3] Contestability is enhanced in the market of those CPSs. This objective is pursued in particular by Article 5(2)(a). To illustrate, a new video-sharing platform service would be better able to compete with the gatekeeper video-sharing platform because the gatekeeper would no longer have the same data advantage as before to attract advertisements: each service would just acquire its own data. It may also improve contestability in the market of AdTech services to third parties as a new entrant in this market is unable to combine the same volume of data as incumbents. Of course, data only gives the gatekeeper one competitive advantage and there are multiple other factors that can affect entry but the DMA considers data accumulation to be a major entry barrier.

Second, Articles 5(2)(b), (c), and (d) seek to improve competition on the end-user side of the platform by facilitating the entry of new services provided by parties other than the gatekeeper. If users do not consent to data sharing, then the incumbent has a less pronounced data-related advantage and new entrants can compete by offering new services on a level playing field. Here contestability is supposed to be enhanced on the platform-to-consumer side of the market by limiting the capacity of a gatekeeper to leverage the data-related advantage it might otherwise have to enter new markets.

Third, **by limiting the capacity of data to be cross used for advertising, this makes the online advertising market more competitive**. This was the theory of harm in *Google/Fitbit* which was addressed by Google committing to create a data silo so that Fitbit's user-generated data would not be used to develop Google's online advertising market at the expense of others.[4] On the facts of that merger, the data could be used for other purposes but these uses will be governed by Arts 5(2)(b) and (c) in the near future.

However, the achievement of the purposes of Art 5(2) can be affected by the gatekeeper securing consent from users to collect personal data. If sufficient users' consent, then the existing market dynamics might not change. This is the most complex aspect of Article 5(2) DMA: **given that gatekeepers whose business model relies on data will probably seek to continue to secure consent**

[2] DMA, Recital 36 clarifies this.

[3] DMA, Recital 56.

[4] Commission Decision of 17 December 2020, Case M.9660 *Google/Fitbit*.

from users, how can this be achieved lawfully? And how far does the DMA constrain this business model? This is the main question discussed here before explaining in more detail what Article 5(2) forbids. Another wider question is whether the consent option risks frustrating this obligation altogether, but this is beyond the scope of this paper.

2.1.2. Content of the prohibition

Article 5(2) prohibits four actions relating to the collection of personal data from users unless there is explicit consent. Personal data means information about an identified or identifiable natural person (the data includes for example: name, location, physical attributes, mental state, economic circumstances, what a person likes and if a person visited a specific website).[5] This kind of data is valuable to advertisers who can offer better targeted ads to users and to platform service providers who can personalise their services or develop new products by understanding consumer demand better. Below we provide an interpretation of the various subsections of Article 5(2).

Art 5(2)(a) prohibits processing personal data of end users which they make available when using the services of third parties who make use of the gatekeeper's CPS if that processing is for the purposes of providing online advertising services.

- The personal data covered by this prohibition may be processed provided it is used for any other purpose. This is different from the other subsections of Art 5(2) which forbid data collection for any purpose. It does not include the use of his data for providing a gatekeeper's own advertisements but this use is regulated by Article 6(2).

- It is not clear what other purposes may be. Recital 36 speaks about developing custom audiences. This would seem to suggest that the data is used to help improve the service offered by the gatekeeper. However, note that the collection and processing of this data for these purposes still requires compliance with the GDPR.

- One should distinguish between (i) a situation where the end-user contract is with a third party but the gatekeeper offers the third-party service, which is covered by Art 5(2)(a) and (ii) a situation where the end-user's contract is with the gatekeeper who also supplies the service, which is covered by Article 5(2)(b) and (c).

- It may be argued that because this provision deals with data obtained when the end-user is using third party services hosted by the gatekeeper, that personal data which the gatekeeper obtains when the consumer uses services of the gatekeeper can be processed for the purposes of advertising. But this would be the wrong conclusion because this kind of data collection is regulated by the other provisions in Article 5(2).

Art 5(2)(b) prohibits combining personal data from the CPS under scrutiny with personal data from any other CPS (whether or not the firm is a gatekeeper in that sector), or any other services provided by the gatekeeper or with personal data from third-party services. This combination of data aims to harvest as much data as possible to identify new services, for example. The combination of data can

[5] GDPR, Article 4(1).

thus strengthen the gatekeeper's core platform service or other services. To a certain extent, even if users consent to combining personal data for the purposes of this provision, it is still the case that the principle of data minimisation in the GDPR applies, which places some limits on what gatekeepers may do with the data and how long they can store the data.[6]

- Unlike Art 5(2)(a), all combinations are forbidden, irrespective of purpose. In fact, this prohibition does not even explain whether or not this data combination is used by the gatekeeper in any way: what is forbidden is simply the combination of this data.
- Implicitly, the third-party services must be those services which use one of the firm's CPSs otherwise it is not clear how the gatekeeper can get hold of the data.
- The purpose of this prohibition seems to be that this data combination strengthens the gatekeeper's position in markets it is present in. For example, the data allows the gatekeeper to personalise a service to the user, or it can make search results more relevant. This benefits the consumer but the legislator is concerned that they also benefit the gatekeeper at the expense of rivals who would otherwise be able to enter the market.

Art 5(2)(c) prohibits the cross-use of personal data from the CPS under scrutiny in other services provided separately by the gatekeeper, including other CPSs.

- The differences with Art 5(2)(b) seem to be two: (1) here data is used, not just combined. However, the distinction between these two notions requires further clarification.[7] One interpretation is that the combination of data refers to a party putting together different data points and drawing inferences from them, while cross-use is about an active utilisation of the data in another market, as provided in the example below; (2) the other service is provided separately.
- The intention might be to address a leveraging scenario like the one addressed using Article 102 in the SEN/ENEL and the Engie cases where the incumbent energy provider used consumer data to enter a newly liberalised market: it had an advantage because it had the contact details of all eligible customers who could benefit from market opening.[8] Adapting this case-law to a digital service, it would mean a scenario where the gatekeeper uses the data to introduce a new service using the data to target this to those most likely to buy it.

Art 5(2)(d) forbids the signing in of end-users to other services of the gatekeeper so as to combine personal data.

---

[6] GDPR, Article 4(1)(c) :

[7] Centre for Information Policy Leadership, Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and
Practical Consequences Discussion Paper (May 2023) pp.13-14

[8] The Engie case was successful (Décision n° 17-D-06 du 21 mars 2017 relative à des pratiques mises en œuvre dans le secteur de la fourniture de gaz naturel, d'électricité et de services énergétiques) but the SEN/ENEL case was not because the data was not commercially significant to give the dominant firm a competitive advantage (*Servizio Elettrico Nazionale v Autoritá Garante della concorrenza e del Mercato*, judgment of the Consiglio di Stato, 1 December 2022).

- This seems to describe one method of combining personal data which is dealt with by Art 5(2)(b).
- It follows that a gatekeeper can continue to provide a single sign-in for multiple services provided data is not combined. If someone does not consent to data combinations set out in Art 5(2)(b) then one may argue they should not be automatically signed in.

2.2. Implementation: How to Secure User Consent to Data Fusion

Article 5(2) allows the gatekeeper to process, combine, cross-use data or sign-in end users to other services to combine data if there is consent by the user. It is very likely that some gatekeepers whose business model relies on data collection will avail themselves of this exception and will try and secure user consent. Therefore, **the assessment of compliance is largely going to focus on whether consent has been obtained lawfully. It is for the gatekeeper to decide how to comply**. However, as we explain below, the DMA appears to indicate a preference for one way of complying. After explaining what that preference is, we show that it is not for the legislator to choose how the gatekeeper elects to comply.

2.2.1. The EU's preferred compliance path

Recitals 36 and 37 suggest one possible pathway to comply. This is just one possible option for gatekeepers, for otherwise the DMA would undermine the freedom of firms to run their business as they see fit as guaranteed by the Article 16 of the EU Charter of Fundamental Rights. The **compliance path found in the recitals** has the following components:

(i) The gatekeeper has to make available **two versions of the same service**.

a. One version is a 'less personalised but equivalent alternative' to the present service;

b. The second version may be described as the 'personalised' where the gatekeeper collects data which, absent consent, would infringe Art 5(2).

The less personalised version should be of the same quality as the version of the service that relies on data collection unless the degradation in quality is a direct consequence of the gatekeeper not being able to process the data. The assumption the legislator makes is that a gatekeeper today offers personalised version' only and so it is expected to roll out a less personalised version. The less personalised version may require the user to consent to handing over data so that the service may be offered in the first place, or the gatekeeper may be entitled to process data lawfully if this data is necessary to perform the contact. But no data that infringes the prohibitions in Art 5(2) may be collected for the operation of this less personalised version.

(ii) Users choose whether to sign up to the less personalised version or the personalised version.

(iii) The gatekeeper may allow the user to **opt in to a more personalised service** by giving consent to data processing. Consent must be sought proactively by providing a user-friendly interface for the consumer to decide whether to consent. Here compliance with

GDPR principles of consent is necessary.[9] Nevertheless the DMA provides some further specifications which impose obligations that may be in addition to those under GDPR:

a. At the time of giving consent the user is advised that even if they do not give consent, the core platform service remains unchanged and no functionalities will be suppressed.[10] In other words, if you do not opt into the personalised version, you can still have the less personalised version;

b. Online interfaces shall not deceive, manipulate or materially distort the ability of the user to give consent;[11]

c. When consent has been refused, a repeat request for consent cannot be made more than once a year.[12]

This is not necessarily the only way to comply. First, Recitals are not legally binding. Second, as mentioned above it undermines the freedom to conduct one's business too far as there may be less onerous ways of complying. Third, it feels commercially unrealistic for some: it assumes that on the day when compliance starts, every user is automatically 'demoted' to a less personalised service and is then asked to consent to a system upgrade by giving over more data. Can this really be what is intended? **Less onerous alternatives can be explored, and some are sketched below. However, it is worth noting that Meta's discussions with the Bundeskartellamt (BKartA) as well as the judgment of the ECJ in *Meta v BKartA* seem to go in this direction**.[13] Both are considered here briefly.

Meta's new accounts centre: users are given the option to combine their various Meta accounts so that Meta could combine the data. The BKartA focused on whether the steps were transparent and comprehensible for the user, whether the process to separate the accounts was sufficiently simple. **Meta is allowed to make it clear that by consenting to hand over data by combining accounts that the user gains additional functionalities, for example cross posting the same user-generated content on two social media platforms. The BKartA makes it clear that a remedy of this nature addresses the competition concerns it identified** but that this is not necessarily a solution that complies with the DMA or new provisions found in German competition law. However, with regards to DMA compliance, it seems clear that the remedy is in line with the compliance pathway envisaged by the DMA.[14]

Meta v BKartA: here the question arose whether Meta's dominant position in the market for online social networks had any role to play in determining the question of consent. While the Court of Justice

[9] The DMA refers specifically to art 4(11) and 7 of GDPR. The elements of consent are discussed elsewhere, see for example EDPB, Guidelines 05/2020 on consent under Regulation 1016/679 (May 2020). See also C-61/19

[10] See for this DMA, Recital 37 and Art 13(6)

[11] DMA, Recital 37 and Art 13(6)

[12] Art 5(2).

[13] Case C-252/21 Meta Platforms v Bundeskartellambt, EU:C:2023:537.

[14] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_Meta_Daten.html

rightly held that dominance does not preclude the possibility of giving consent, **market power was relevant to assess if content was freely given**.[15] The Court linked this factor with Article 7(4) GDPR:

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

With reference to the facts of the case, the ECJ thought that the processing by Meta was not 'strictly necessary' for the performance of the contract between Meta and users.[16] It follows that users should be free 'to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.'[17] Here too the hint (it can only be a hint because the ECJ cannot answer questions of fact in a preliminary ruling) is that a **dominant firm wishing to secure user consent to data must offer an alternative way of accessing the service to one that requires the consent to handing over data**.

However, there must be other ways for gatekeepers to comply with Article 5(2) and some options are discussed below.

2.2.2. What less onerous alternatives might be considered?

A first option would be that, on the date when compliance is due (i.e. six months after the gatekeeper designation), **the gatekeeper gives users a take it or leave it offer**: you may use this service if you continue to consent to data collection or you are no longer entitled to the service. After all, neither the DMA nor any general principle of EU law compels a firm to do business with any user unless there is a specific obligation imposed by law.

To a certain extent, the judgment in *Meta* seems to run counter to this intuition because it assumes that for the purposes of ensuring that the user consents freely (based on a joint reading of Article 102 and the GDPR), she must have a choice between two viable options to contract with the gatekeeper: by handing over data or by not handing over data. This is a striking interference into freedom to run one's business: it seems that dominant firms cannot provide a product that relies on extensive data extraction if the user cannot obtain that product without handing over data. This results from a joint reading of Art 102 and GDPR and is not an innovation brought about by the DMA, which does not impose a requirement to offer a less personalised and a personalised version for the user to select. However, it is arguable that since the DMA makes reference to the GDPR and that most likely a gatekeeper enjoys market power akin to dominance, that the holding in Meta can be transposed to the DMA. If so, then a take it or leave it option is not feasible. It might even be challenged as contrary to the spirit of the DMA which is to facilitate user choice rather than prevent it.

[15] Meta (above n 13), para 148

[16] Meta (above n 13), para 149.

[17] Meta (above n 13), para 150.

A second option could be for the **gatekeeper to offer a paid-for service where data is not processed** in ways contrary to Article 5(2) and a free service in exchange for data. A question arises if the price of the paid-for service is too high whether this would be read, following the *Meta* judgment, as de facto not a choice at all, and so contrary to Art 102 TFEU.[18] However, it may be consistent with the DMA.

A third option could be for the **gatekeeper to buy user data**. After all, the economic value of the gatekeeper is in part sustained by its users clicking and staying on the platform as long as the platform can retain their attention. Nothing prevents this under the DMA: consent is obtained when the user agrees to be remunerated for agreeing to have their data used, but it is not likely that a gatekeeper would consider this option.

A fourth option, the rationale for which will become apparent in section 2.2.3 below, is **that the gatekeeper provides one less personalised service and then a range of more personalised services**, each of which requires that the user consents to some data being used. For example, a slightly more personalised service if the user consents to allow the data to be combined with other data, a more personalised one if the user consents to the data being used for advertising purposes and so on.

In sum, as a matter of law, the DMA cannot compel a firm to design its business in a specific way. It can only forbid certain business models when these are inherently contrary to the DMA provisions. Within that parameter, a gatekeeper has a certain leeway in choosing how to comply. Some options were canvassed here as a way of illustrating the various options available. The common denominator is that whatever option is adopted, the user must consent and this leads us to discuss how gatekeepers should be expected to make choice possible.

2.2.3. How to design the end-user's choice?

One difficulty in implementing any of the approaches sketched above is that **the gatekeeper has to inform the user of multiple data collection practices where that arises**. The user should opt in to each one. An end-user for example may be willing to consent to data being processed for advertising purposes (Art 5(2)(a)) but may want to deny giving consent for the other two purposes in Art 5(2)(b) and (c). So, then a **gatekeeper has to offer a menu of consent options when providing the so-called 'personalised service'. Alternatively, the gatekeeper can present individual choices at different times and not all at once.** This would seem to be the requirement under the GDPR.

Here there is a tension. Consider a gatekeeper who offers two options: a less personalised option and a personalised one, where all data collected for all purposes in Art 5(2). This might not satisfy the DMA requirements because the user's choice is not sufficiently specific, and this may not be sufficient for the purposes of the GDPR either. However, the user might understand this choice relatively easily and decide if they are happy for data to be used.

Consider instead a gatekeeper that offers a less personalised version and a personalised option where the user decides which data uses it consents to, one tick box for every provision in Art 5(2)(a), (b), (c)

[18] For discussion see F. Scott Morton, 'Meta's Offer' VoxEU Column 13 December 2023.

and (d). This allows the consumer to give specific consent, but will a user read this, and if they do will they understand the implications of each choice?

In sum, the point we suggest here is that offering just two options, a less personalised one without data collection and a personalised one with all data collected, may be a choice a user understands well and can make a decision in an informed manner. Conversely, a choice that asks the user to give specific consent to each and every use of data may be one that users do not understand as clearly and may not make choices that represent their preferences. In sum, the DMA might be more effective if two options are presented, but the gatekeeper is more likely to be compliant if it offers a less useful choice menu with multiple choices. While this interpretation runs counter to the idea of consent embedded in the GDPR and the DMA, some realism is needed on the part of the enforcers: we cannot regulate on the assumption that users have high levels of literacy and read every word attentively when asked to consent.

This is where a trade-off is needed: a solution which on paper maximises user choices but it is overly complicated for users to understand means that many users risk making choices that do not correspond with their preferences. Conversely, a more modest set of choices may not be perfect but the user would be able to understand what they are choosing. Effectiveness as a general principle might indicate that the latter is a preferable solution.

There may be a long-term solution, drawing on how user choice has been simplified in other fields. For example, since we know that consumers do not read or understand how unhealthy certain foods are a **simple labelling system** is used to indicate calories in food (red, yellow, green). For white goods energy consumption standards are simplified with energy labels because few consumers would understand the numbers provided by manufacturers. Might a similar approach be used for gathering data consents for the purposes of Article 5(2)? It is beyond the scope of this paper to discuss this fully but briefly one might imagine a scenario where a gatekeeper labels its choice options along a scale the colours serving as a proxy for the amount of data you hand over (green no data collected, red all data collected), or industry participants can agree on setting standards for data use, or the EU can legislate to set these.

The literature assessing labels for food content and energy consumption gives mixed results: policymakers seem to agree that this can be a helpful measure but the evidence suggests that the design of these simple information tools is difficult and that they may affect certain classes of consumer above others. For example, one study reveals that the EU energy label does not increase demand for energy-efficient goods while information about the lifetime costs of operating the goods increases demand for energy efficient products.[19] However another study finds the opposite.[20] These differences are explained by a third study which concludes that 'the specific national context in which

[19] M.A. Andor, A. Gerster, L. Götte, 'How Effective is the European Union Energy Label? Evidence from a Real-Stakes Experiment' (2019) Environmental Research Letters 14 044001.

[20] M. Skourtos et al 'Efficient Energy Labelling : The impact of Information Content and Style on Product Choice ' (2021) 14 Energy Efficiency, Article number 58.

an intervention is implemented is a key determinant of its effectiveness.'[21] Another reviewing several studies points out that nutrition labels have little effectiveness among people in a low socio-economic position.[22] The takeaway is that **effective design is a challenge but it seems to provide better results than not providing consumers with the capacity to make choices based on simple heuristics**.[23]

2.2.4. The contents of a less personalised version

Another difficulty that arises should a gatekeeper decide to roll out a less personalised service is working out what a lawful less personalised service consists of. Given that many gatekeepers have been offering services with extensive data collection, **how can one determine if the less personalised service is of an appropriate quality** or if the gatekeeper has degraded the conditions or quality of the CPS provided to users who avail themselves of the rights in Article 5(2)?

Consider for example cross-posting, the practice of making it possible for a user to post the same content simultaneously on two platforms owned by the gatekeeper. Suppose that in pre-DMA times all users had the ability cross-post but data was collected and combined. The gatekeeper now designs a less personalised version of the service without data collection: must this basic version allow for cross-posting or can cross-posting be only made available if the user consents to some data sharing? Further discussion of this question probably requires us to know more about how a platform works, but a reasonable assumption is this: in order to make cross-posting happen, the platform necessarily has to have and use some personal data from the user so that it can match the user's two accounts. It is likely that the gatekeeper must, using the terms in Art 5(2)(c), cross-use some personal data. So, in this way, **cross-posting is definitely not a part of the less personalised service** because that service must be available without collecting some data forbidden by Art 5(2) DMA and the gatekeeper must ask for user consent.

One more key observation may be made drawing on the example above: assume that the gatekeeper proves that it cannot offer cross-posting under the less personalised service because it can only offer it by cross-using personal data. This does not mean that the gatekeeper, when offering the user the option to opt in to the personalised service which includes cross-posting, is limited to seeking consent for those uses forbidden by Art 5(2) which are necessary to offer the service. The gatekeeper is free to offer the more personalised service on condition that the user gives consent to all data collection prohibited by Art 5(2), subject to the discussion above regarding the need for consent to be specific and subject to compliance with GDPR principles.

These interpretations of Art 5(2) are summarised in a more general manner in the table below.

---

[21] S. Ceolotto & E. Denny, 2021. 'Putting a new 'spin' on energy labels: measuring the impact of reframing energy efficiency on tumble dryer choices in a multi-country experiment' Trinity Economics Papers tep1521, Trinity College Dublin, Department of Economic

[22] D. Sarik et al 'The Impact of Menue Energy Labelling Across Socioeconomic Groups : A Systematic Review (2016) 99(1) Appetite 59.

[23] See generally M.A. Andor et al, 'Consumer Inattention, Heuristic Thinking and the Role of Energy Labels' (2020) 14(1) The Energy Journal 83.

Determination of less personalised service	The gatekeeper can defend the provision of a less personalised service that lacks features available on the premium version by showing that the feature in question can only be offered if the user consents to the collection of some data otherwise forbidden by Article 5(2).
Scope of consent for the **personalised service**	The gatekeeper is free to require that the user consents to all data processing otherwise forbidden by Art 5(2) and is not limited to asking for consent for data processing necessary to deliver the personalised service.

The justification for these two interpretations (which might at first blush seem contradictory) should be clear. The less personalised service is defined by the DMA itself as a service that does not rely on data uses forbidden by Art 5(2). However, the burden of proof is on the gatekeeper to show that it cannot offer the service in question without using personal data listed in Art 5(2). This is where the compliance report can provide valuable information: it allows the gatekeeper to reveal how the platform works and what data is necessary to ensure that a service functions.

When it comes to the scope of consent, Article 5(2) does not limit the type of data use that the gatekeeper can ask consent for or make that depend on what additional services can be provided with that data. However, it is arguable that the DMA requires that the gatekeeper explains to users the services that can be provided to them or the benefits they might receive indirectly if they consent to the collection and use of data.

2.2.5. Data fusion under Arts 6(1)(c),(d) and (e) GDPR

The DMA provides that a gatekeeper can also combine data on three other legal bases and the judgment in *Meta v BKartA* helps interpret each. These alternative legal bases are unlikely to be relied on frequently.

*Article 6(1)(c): processing is necessary for **compliance with a legal obligation** to which the controller is subject.*

Meta seems to have argued that it had a legal obligation 'to collect and store personal data in a preventive manner in order to be able to respond to any request from a national authority seeking to obtain certain data relating to its users.'[24] This would be something for the national court to consider.

In addition, the Court states that this is a legitimate legal basis only '(1) where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, (2) where that legal basis meets an objective of public

[24] Meta (above n 13), para 132.

interest and (3) is proportionate to the legitimate aim pursued and (4) where that processing is carried out only in so far as is strictly necessary.'[25]

*Article 6(1)(d): processing is necessary in order to **protect the vital interests** of the data subject or of another natural person*

The Court in Meta draws on Recital 46 GDPR to suggest that this provision deals with the protection of the life of the data subject or another natural person. Here 'in view of the nature of the services provided by the operator of an online social network, such an operator, whose activity is essentially economic and commercial in nature, cannot rely on the protection of an interest which is essential for the life of its users or of another person in order to justify, absolutely and in a purely abstract and preventive manner, the lawfulness of data processing such as that at issue in the main proceedings.'[26]

*Article 6(1)(e): processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.*

The question in Meta was whether it was 'entrusted with a task carried out in the public interest or in the exercise of official authority, in particular with a view of carrying out research for the social good and to promote safety, integrity and security.'[27] While this was for the national court to find out, the ECJ considered it was unlikely to apply.

In addition to providing guidance on the possible meanings of these three provisions, the Court insists that because data processing on **these legal bases is non-consensual that they must be interpreted restrictively**.[28] The burden rests on the gatekeeper to demonstrate that data combination or cross-use are necessary to achieve these goals. However, some have suggested that these legal bases are too narrow to protect users adequately.[29]

However, the **gatekeeper who wishes to take advantage of these alternatives cannot collect data for all the four uses forbidden by Art 5(2)**. In other words, based on the principle of proportionality the gatekeeper has a duty to show which data it must collect or use in order to discharge the obligations in Articles 6(1)(c), (d) or (e). For example, if the gatekeeper states that processing 'is necessary for compliance with a legal obligation to which the controller is subject' then it has to explain which of the forms of processing forbidden in Article 5(2) it must be allowed to carry out. It seems difficult to imagine a scenario where the legal obligation would require that the gatekeeper processes data for the purposes of providing online advertising forbidden by Art 5(2)(a) but it may be that combining personal data of user from multiple platform services is necessary if there is legislation requiring, for example, that a social media provider collects all data about user online activity. However even here this collection of data on user activity cannot be used to secure a competitive

[25] Meta (above n 13), para 138 (numbers added for clarity).
[26] Meta (above n 13), para 137.
[27] Meta (above n 13), para 133.
[28] Meta (above n 13) para 93.
[29] See some examples and discussion by Centre for Information Policy Leadership (above n 7) pp.16-19.

advantage. Thus, these three additional legal bases allow the collection of data for reasons that are not going to affect fairness or contestability.

2.3. Relationship with Other EU Legal Provisions

2.3.1. Between Art 5(2) and Art 15 DMA on auditing profiling techniques

Article 15 requires that gatekeepers perform an audit of techniques for profiling consumers that are applied in the CPS. This is transmitted to the European Data Protection Board and the gatekeeper must also provide a publicly available overview. It is not clear how this reporting obligation helps the enforcement of the DMA. However, the intention behind the public report is to facilitate contestability: by making it more transparent for users how the gatekeeper collects and uses their data, this can make it possible for 'other undertakings providing core platform services to differentiate themselves better through the use of superior privacy guarantees.'[30] It can be doubted that these reports are valuable for end-users to gain a better understanding of what their data is used for and thereby strengthen their capacity to consent. Some consumer organisations may use these to facilitate user understanding though.

However, the DMA does not require a shift to a data collection-free market for any core platform service. Rather, it creates the possibility for competition to emerge based on privacy settings. It does not stop a new entrant from competing against a CPS by itself gathering as much data as is lawfully possible. The legislation is agnostic about which business models might emerge once markets become more contestable. This matters: laws can encourage the development of preferred market outcomes but very rarely do laws ban certain markets out of existence.

2.3.2. Relationship with other EU rules

Article 5(2) creates a system whereby when the gatekeeper secures consent, it does so in a manner that is GDPR compliant. As discussed above it seems that **in order to collect data covered by Article 5(2) by securing user consent, the DMA imposes further procedural requirements**: the gatekeeper cannot ask for consent repeatedly; the gatekeeper cannot use dark patterns to secure consent; refusal to consent cannot deprive the user of a service without data collection.[31]

It is worth stressing that the **DMA is not some sort of GDPR+ regime** such that the fundamental rights of data subject are protected better because of the DMA. The purpose of the DMA is not to enhance the rights of data subject. This objective may nevertheless be achieved indirectly because the DMA adds the procedures summarised above to gatekeepers and because it stimulates the emergence of business models that rely less on personal data.

[30] DMA Recital 72.

[31] See also ICO, CMA and DRCF, Harmful Design in Digital Markets : How Online Choice Architecture practices can undermine consumer choice and control over personal information (9 August 2023). https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf. See also Amelia Fletcher's paper in this series.

3. ARTICLE 6(2) DMA

3.1. Purpose and Interpretation

3.1.1. Purpose

This provision is based mainly on the contestability aim of the DMA. It may also be explained as being about fairness because otherwise the gatekeeper takes advantage of data which has been generated thanks to business users. It is designed principally to level the playing field in markets where the CPS offers a distribution service for business users to reach consumers. Gatekeepers who use the data of the business users that are present on its platform are able to leverage into the market occupied by those business users, and Art 6(2) prevents this. Thus, the market where this obligation **creates contestability is the market for goods or services provided to end users through the CPS**. This is perhaps surprising because this could be any market, not necessarily a digital one.

Whether Art 6(2) **may also make any of the CPS markets more contestable is less certain** although it is possible that a disruptive innovator begins by relying on the CPS to gain scale and then becomes itself a CPS. For example, a firm making widgets might start selling these on Amazon, but it may then gain sufficient numbers of customers that its website becomes the go to place for buying widgets and other widget producers ask to sell their goods on that platform in preference to Amazon. Amazon, unable to use that business user's data, cannot compete against it in the widget market as easily as it could before this obligation came into force. However, it is not clear that Article 6(2) on its own can contain a gatekeeper to such an extent that a rival can enter the CPS market.

3.1.2. Interpreting the obligation

*What is the obligation about**?***

Users of gatekeeper services generate data while using the CPS. Some of this data is personal data generated by customers of the business users. This data becomes accessible by the CPS in order to facilitate the transaction between the business user and the consumer. Data may be discrete: about a specific transaction (Joe Bloggs bought a Barbie doll on 1 June 2023) or aggregated (based on the transactions on the platform, consumers in the UK aged between 40 and 50 buy a lot of Barbie merchandise and pink goods). This data can be useful for the business user because they can gauge demand and develop new products. In the hands of a gatekeeper, this data allows it to leverage its position into those markets where there is demand. Obviously if the same data is also available publicly, then the gatekeeper is free to use that public record.

To which CPS does this provision apply?

Some are clearly within the scope: app stores, marketplaces, virtual assistants. Less clear if this also applies to search, advertising or social networks. The test is whether there are business users that rely on the CPS to offer goods or services downstream.

Recital 46, final sentence reads: 'That obligation should apply *to the gatekeeper as a whole*, including but not limited to its business unit that competes with the business users of a core platform service.' This means that the **obligation applies to all the gatekeeper's entire line of business, all the core**

platform services that it operates but also, it seems, any other lines of business. This is necessary because if the idea is to prevent leveraging data, then this risk is mitigated only if that data may not be used for the purposes of competing with the business user. It means the obligation applies to the enterprise as a whole, beyond the technology segments identified by the DMA.

What data?

The text is drafted to encompass a wide range of sources of data by including both data generated by the business user or by the consumer using the services of that business user. It does not seem that the data need necessarily lead to a transaction being concluded between the business user and the consumer, thus search data is within the scope.

Data which is subject to this obligation must be '**not publicly available**.' The burden of proof should be on the gatekeeper to reveal that the data is available elsewhere and not on the business user to show this. After all the presumption should be that the data about how frequently consumers search or buy a particular good is not available to the public.

Finally, on the concept of data, consider these questions:

1. The data cannot be used 'in competition with business users.' This raises a question about whether these are actual or also potential competitors. For example, the business user sells a mousetrap through the CPS and the gatekeeper uses that data to develop a trap for cockroaches using that data. Is this illegal use of the data?

2. Is old data outside the scope? Can a gatekeeper say that data gathered 5 years ago can no longer serve to give it a competitive advantage?

3. what about data from past business users?

These questions raise an issue about how to interpret the DMA. A **literal reading would allow to give a fairly broad interpretation** in some cases (all business users, past and present and even old data), and if this is over-inclusive this is irrelevant because the purpose of the DMA is to make application as clear as possible, Type 1 errors are accepted. Conversely, a **purposive reading would allow to narrow down the scope** of the data to be 'siloed' by claiming that some data is not valuable for the purposes of leveraging.

But to make matters trickier, a purposive reading could also help widen the scope of data for example by extending it to potential competition because the aim is to make markets contestable and allowing the gatekeeper to use data to develop new products enhances the gatekeeper's power at the expense of rivals. This may be supported by the importance to stimulate dynamic competition which is served by offering business users a wide range of data so that they may discover new products.

One caveat may be entered: if the gatekeeper makes the data publicly available, then the data is no longer subject to this obligation. Might it be to a gatekeeper's interest to make such data publicly available so that it too may use it? For example, aggregated data which does not identify users and

therefore is not subject to GDPR protections could be published and then it could be used by both business users and end users.

Which business users benefit from Art 6(2)?

The answer is on the whole fairly clear: **those who use the CPS, but some borderline cases** are worth exploring: (i) business users who have been terminated by the gatekeeper for legitimate reasons (e.g. a business user who does not comply with the gatekeeper's terms and conditions); (ii) business users who have stopped using the CPS, because they have opted to use another CPS to offer their goods/services? How to decide if these are to be included?

3.2. Implementing the Obligation

The shorthand for Art 6(2) is that this is a provision about creating 'data siloes'. This description is a little too simplistic because the silo is composed of data for a specific purpose. Data generated by a business may be used legitimately by the gatekeeper (e.g. to improve a search function on the platform). These legitimate uses are pro-competitive because the gatekeeper uses data to rank results in a manner that is favoured by consumers. However, recall that if the gatekeeper processes personal data in order to achieve this, it must have a lawful basis under the GDPR.

It follows that it is important to be clear that it is **only *specific uses of the data* which are forbidden and placed in a silo**. It follows that this is not a rule that prohibits the gathering of such data. This has implications for the enforcement of this obligation.

The only way to verify compliance would be to offer access to the data management plans of the firm so that the use of the relevant data can be audited: who is given access to it, in which workflows does the data go? Are there clear and fail-safe protocols to ensure that the data does not flow to that business unit which might use the data to develop goods/services that compete with those of business users?

A useful model for what is expected may be the data remedy in *Google/Fitbit*.[32] Space prevents a full account, but these are the key points from that decision that also apply to DMA compliance which reveal that these commitments hold some information about how the Commission may wish to see the DMA implemented:

The identification of the data and the definition of the scope of uses that is out of bounds as well as which Google workers who may access the data for other legitimate purposes.[33] The decision reveals that this needs to be specified carefully. For example, the commitment includes 'the obligation to compile specific and detailed access documentation in relation to individuals and services that will have access to the relevant data, in order to facilitate the monitoring of Google's compliance with the related obligations. Minimum data and information points subject to periodic audits are also introduced. The improvements appear able to limit the risk of circumvention and of misuse of the

[32] Commission Decision of 17 December 2020, Case M.9660 *Google/Fitbit*.

[33] The Commission speaks of a 'strictly permissioned data storage environment' that holds the data and of 'strictly permissioned temporary logs' which hold the data for specific and permitted processing facilities. Ibid., para 862.

relevant data and in case give the Monitoring Trustee an increased ability to deter violations and to address them.'[34]

Having a Monitoring Trustee who is technically capable of checking that there is compliance and that they have access to 'the technical means through which data separation is granted.'[35]

Moreover, the Monitoring Trustee should be able to assess 'the adequacy of the technical means through which data separation is obtained.'[36]

In turn, it follows that the Monitoring Trustee must have adequate technical abilities and expertise.

Specifying that Google may change the technical means to comply with the data separation commitment as new technologies and standards evolve, with the proviso that changes are supervised by the Monitoring Trustee.[37]

It seems that for the purposes of the DMA the monitoring function is for the compliance function unit. Furthermore, from a procedural perspective, it seems that this remedy is probably best designed with stakeholder input and with a steer from the Commission.

3.3. Relationship with Other EU Legal Provisions

3.3.1. Between Art 6(2) and Art 5(2)

These two data-related obligations work **independently of each other**. The simple fact that the gatekeeper has obtained the consent of the user under Article 5(2) does not allow the gatekeeper to use that personal data for the purposes listed in Art 6(2).

To make this more concrete: The user logging on to a CPS transmits personal data directly to the gatekeeper. The gatekeeper might well obtain consent under Article 5(2). However, this cannot allow the gatekeeper to use this data for the purposes of Article 6(2). The prohibition in Article 6(2) is *per se*: no user consent can override it. Any other reading would make Article 6(2) easy to circumvent.

3.3.2. Between Art 6(2) and 6(10)

Article 6(2) **forbids the gatekeeper** from accessing certain data. Article 6(10) requires the gatekeeper to **provide data to** business users.

Article 6(10) includes the same data as Art 6(2) (i.e. that which is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services) but it also includes personal data generated or provided by 'end users engaging with the products or services provided by those business users.'

[34] Ibid., Para 966(e). See also para 897 for a detailed list of points to be defined.
[35] Ibid., Para 959
[36] Ibid., Para 967(b)
[37] Ibid., Para 863

3.3.3. Relationship with other EU rules

Perhaps for completeness Art 6(2) includes personal data, but any GDPR compliance measure is irrelevant for the purposes of interpreting this obligation, except for the question whether the gatekeeper can use that personal data for purposes other than competing with business users, in which case that use would have to be lawful under this provision but falls to be regulated by Art 5(2) and the GDPR.

However, it must be made clear that **Article 6(2) has nothing to do with the GDPR duties**: the data subject has no rights under Article 6(2) of the DMA. However, the gatekeeper might have some GDPR duties nonetheless. For example, if the consumer buys a good form a gatekeeper platform which is sold by a business user of the gatekeeper, then some data about the consumer has to be transferred from the business user to the gatekeeper to complete the contract. There are GDPR obligations in this relationship, but these operate independently of the DMA. The gatekeeper platform may be a joint controller and have to demonstrate a legal basis for processing the information.

Finally, the notion of 'use' under this provision of the DMA is not based on this use being lawful or unlawful under GDPR: use is illegal when the data is processed to gain an economic advantage over a rival.

4. DATA PORTABILITY AND ACCESS FOR END USERS AND BUSINESS USERS: ARTICLE 6(9) AND 6(10)

4.1. Purpose and Interpretation

Next to the prohibitions, the DMA imposes also obligations related to data access and sharing. This paper focuses on the two data portability and access obligations benefiting end-users (Art.6.9) and business users (Art.6.10). [38]

First, Article 6(9) augments the data portability right of the GDPR and provides that:

The gatekeeper shall provide **end users and third parties authorised by an end user**, at their request and **free of charge**, with effective portability of **data 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, including by providing, free of charge, **tools** to facilitate the effective exercise of such data portability, and including by the provision of **continuous and real-time** access to such data. (our underlining)

Recital 59 clarifies the objective of the obligation which is related to the general objective of the DMA (i.e., market contestability and distributional fairness) in the following way:

> *(…) to ensure that gatekeepers do not undermine the **contestability** of core platform services, or the innovation potential of the dynamic digital sector, by **restricting switching or multi-homing** (… which) should lead, in turn, to an increased choice for end users and acts as an incentive for gatekeepers and business users to innovate.* (our underlining)

[38] This part draws on J. Kramer, Data Access provisions in the DMA, CERRE Report, January 2023.

Second, Article 6(10) creates a new data portability right for business users and provides that:

The gatekeeper shall provide **business users and third parties authorised** by a business user, at their request, **free of charge**, with effective, **high-quality, continuous and real-time access** to, and use of, aggregated and non-aggregated data, including personal data, that is **provided foror generated** in the context of the **use of the relevant core platform services or services provided together** with, or in support of, the relevant core platform services by those businessusers and the end users engaging with the products or services provided by those business users.

With regard to **personal data**, the gatekeeper shall provide for such access to, and use of, personal data **only where the data are directly connected with the use** effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users **opt in** to such sharing by giving their consent. (our underlining)

The objective of this second portability obligation is not explicitly clarified in the DMA, but the obligation contributes to (i) contestability as it facilitates business users switching and multi-homing, (ii) innovation as it stimulates data-driven innovation by business users and (iii) fairness as business users would be more control of 'their data'.

Thus, the "data mobility" stimulated by the new DMA data obligations would increase contestability, fairness and ultimately innovation on the EU digital markets. However, it is absolutely key that this new data mobility does not undermine data privacy and security and ultimately the trust of the users in the (big and small) providers of digital services and, more generally, in the digital society. For this, privacy and security risks should be managed carefully by all stakeholders involved in the increased data mobility framework and users should be educated to the possibilities and risks of these new choices.

4.2.Implementing the Obligations[39]

The data portability and access obligations create optional choices for end and business users, and therefore it would be important that the **choice architecture follow the legal and economic principles specifically mentioned in the companion paper on choice architecture i.e. effectiveness, proportionality, non-discrimination as well as the 'Attend, Access, Assess Act' choice framework, ex ante testing and ex post assessment**.

Besides those principles applicable to choice architecture, the implementation of the data related obligations should also respect three general good regulatory principles: effectiveness and proportionality, participation and non-discrimination.

4.2.1. Effectiveness and proportionality

[39] J. Krämer, P. Senellart and A. de Streel, Making data portability more effective for the digital economy, CERRE Policy Report, June 2020 and R. Feasey and A. de Streel, Data sharing for digital markets contestability, Towards a governance framework, CERRE Report, September 2020

The implementation of the data related obligations should be based on two main general EU principles:

The principle of *effectiveness* is a general principle of EU law and is also mentioned generally in the DMA (Art.8.1 with sets out a double effectiveness principle, with regard to the data portability obligation and with regard to the DMA twin objectives) and specifically mentioned for each data portability obligation;

- The principle of *proportionality* which is also a general principle of EU law
- **To ensure effectiveness, the data portability and access should be properly managed**. The data transfer needs to be secure, minimising risks for data leakage to parties not involved in the transfer, data modification or loss of data.

In particular, it is key that the authorised third party receiving the user's data under Article 6(9) can be trusted and must adhere to the GDPR and adequately protect the data in their respective systems, not only during the transfer, but after the transfer takes place. Furthermore, authorised third parties should be expected to use the data for the purposes underpinning 6(9), which are for switching and multihoming and should not sell/further transfer/use the data for other purposes without expressly informing users prior to any transfer. Without implementing independent harmonised privacy and security standards/verifications that third-parties ought to meet before they entice users to port their data and begin pulling their data from gatekeepers, the risks to data security of EU citizens increase.

Moreover, experience of the implementation of previous portability obligations, such as number portability between telecommunications operators or data portability between financial institutions within the context of Open Banking[40] suggests that there are **opportunities for the data holders to hinder the transfer**. Thus, a prerequisite for the effective implementation of new data portability obligations will be trust on the part of the business and end users who stand to benefit from it. Unjustified actions that create unreasonable doubt or uncertainty about the reliability of the process, or the risks involved, will tend to favour the gatekeeper and reduce the volume of transfers that occur.

As explained in Kramer et al (2020), there are **various data models and formats** commonly used in the digital economy: 'These formats can be roughly categorised as structured, semi-structured and unstructured data. In both the structured and semi-structured cases, file formats only specify a syntactic layer on how information is represented. To make sense of it, it is necessary to know the schema of the data, i.e. what fields and data attributes exist, and what constraints on the data values should be respected. Beyond the syntax (provided by the file format), the schema and the constraints (given by the schema annotations, when available), data needs to be interpreted with respect to a specific semantics, which gives meaning to data fields and attributes. When data is exchanged between two data controllers using different schemas, it is necessary to transform it from one schema

[40] Fingelton/Open Data Institute note that under the Second Payment Systems Directive, users are required to fully re-authorise their permissions every 90 days. Although ostensibly to reaffirm customer consents and retain customer control, this provides an incumbent platform with a periodic win back opportunity: 'The current PSD2 legislation requires a full reauthorisation every 90 days, which can make Open Banking products cumbersome for users and lead to user attrition for TPPs, increasing costs for them'. They suggest a cost benefit review is undertaken to assess the merits of this obligation.

to the other, using schema mappings from the source to the destination. These schema mappings are, most of the time, handwritten by data engineers, although there is sometimes the possibility of automated learning from examples.'

In that regard, the DMA provides that the gatekeeper will have to set up technical tools for an effective portability of data in continuously and real-time manner combined with the protection of privacy, security, and service integrity.

Recital 60 clarifies that the appropriate technical measures could:

- *consist of high-quality application programming interfaces or integrated tools for small volume business users.*

As mentioned by Kramer (2023), it will be important to **harmonise data formats and interfaces for data portability across the different gatekeepers** so as to allow third- party tools, such as Personal Information Management Systems (PIMS), to better integrate with the largest possible set of firms and thereby to facilitate switching and multihoming. In other words, instead of having one tool per gatekeeper, it would be better to have one tool that is able to connect to all gatekeepers for the purposes of data portability.

When personal data are involved, an additional difficulty is the establishment of a **consent management** system which is effective and respect the GDPR requirements of Art.7 GDPR. Indeed, Recital 60 clarifies also clarifies that:

a gatekeeper should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required.

This relates to the **granularity** of consent but may also includethe possibility to give **automated consent**, for instance, through tools such as Personal Information Management Systems.

The consent management system will also require an effective **process of for user authentication.** As noted by Feasey and de Streel (2020), large digital platforms already offer their authentication services to third-party platforms which allow their users to connect to those platforms without the need to re-authenticate. Hence, the adoption of fingerprint, eye or facial recognition as a means of authenticating consents for data transfers might be leveraged if these firms are involved in the process. Regulatory oversight may be required to ensure that it is implemented in a manner which both safeguards the interests of users and achieves the objective of promoting competition.

4.2.2. Participation

The **process and technical tools could be determined by the gatekeepers** who know their products the best and can choose the most proportionate tools. However, to alleviate the risk that the gatekeepers undermine the effectiveness of the data portability, the establishment of those mechanisms should be done **in close partnership with representatives of the beneficiaries of those obligations** and under the supervision of the Commission. In reviewing gatekeeper submissions, the Commission could seek input from third-parties (including those representing consumers) and draw on the evidence collected by gatekeepers through A/B testing. The Commission could usefully also set out

how it expects gatekeepers to engage with third parties too as explained in the companion paper on DMA process and compliance.

In particular regarding the development of **technical standards that ensure an effective and security and privacy preserving data transfer**, experience suggests that this is best regarded as a process rather than being a discrete event. Therefore, the Commission could play an important role in convening the technical forum in which common standards for APIs and integrated tools would be developed in a manner that fairly balances the interests of all parties, and ensuring that there is an appropriate representation of interests without the process becoming unmanageable.[41] Examples may be drawn from the Australian Consumer DataRight (CDR) initiative, which has also relied on a standardisation body.[42]

This process could seek to build upon work done by the *Data Transfer Initiative*[43] since this already involves a number of gatekeepers, and the Commission would need to ensure that all interests are properly represented and that the resulting outputs do not enable gatekeepers to impose unreasonable costs on others.

Finally, several studies on data sharing arrangements that require the consents of end users place emphasis not only on the ease of using the data transfer process itself but also on the need for policymakers or regulators to **educate and inform users about the benefits of their doing so as well as the control of the risks in terms of privacy and security.**[44] Even if an end-user benefits in terms of being able to switch between platforms, many users may not be aware of their rights. The Commission may ensure that the gatekeeper inform users of their rights and risks or even to inform potential entrants of the opportunities that are available to them.

4.2.3. Non-discrimination

Finally, when there is a relevant benchmark in the internal operations of the gatekeepers, the tools offered by the gatekeepers for data portability to third parties should be non-discriminatory. For instance, in the context of the Revised Payment Services Directive (PSD2 Directive), performance and reliability of the interface used for data portability was measured against the data provider's other consumer-oriented interfaces.[123]

4.3. Relationship with Other EU Legal Provisions

The **data portability obligation of Article 6(10) DMA is complementary to the data siloing of Article 6(2)**; while the latter aims to create a level playing between the gatekeepers and their business users, the former aim to facilitate switching and multi-homing. Both provisions benefit the same business users and a similar scope of data.

[41] DMA, Art. 48 and Rec. 96

[42] https://www.cdr.gov.au/

[43] https://dtinit.org/

[44] Ctrl-Shift (2018), p.12: 'Consumers have a lack of know-how and understanding of the digital market, and limited knowledge about their data, how it is used, and how they could use it. This makes the individuals vulnerable to abuse and lacking in the skills to access the opportunity'.

The **data portability obligation of Article 6(9) DMA is also complementary to the GDPR**. Both legal provisions have different objectives as the former reduce users switching costs will the latter aims to ensure the self-autonomy of the users. However, Art.6(9) DMA complements Art.20 GDPR[45] by imposing obligations which go further (data should be given continuously and in real time, free tools to facilitate the effective exerciseof data portability …) but only on designated gatekeepers. It is thus important that both the DMA and the GDPR are applied in a complementary manner, through a dialogue between the authorities in charge of the GDPR (the national data protection authorities) and the authority (the Commission) in charge of the DMA within the DMA High-level group.

[45] As expressed by Recital 59.

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