Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Data Sharing Obligations Under the DMA: Challenges and Opportunities

CIPL Discussion Paper | May 2024

Table of Contents

Data Sharing Obligations under the DMA: Challenges and Opportunities

The Centre for Information Policy Leadership (CIPL)[1] has been at the forefront of promoting responsible use of data for more than 20 years. As such, CIPL supports the goals of the European Union's (EU) Digital Strategy, fostering innovation, growth and competitiveness in the EU while establishing safe and trusted digital spaces for individuals. Building on our work on accountability and effective data protection and as part of CIPL's ongoing project examining the digital legislation package[2], we are publishing a series of papers that examine potential implementation challenges and remaining legal uncertainties concerning the Digital Markets Act (DMA).

In the first paper, CIPL provided an overview of the data protection implications of the DMA.[3] A second paper took an in-depth look at open questions regarding the DMA's seeming limitation of legal bases available for certain processing of personal data for *data combination* and *cross-use* of personal data. This third paper analyses the operational consequences of the DMA obligations for gatekeepers and organisations receiving or getting access to personal data, specifically in the context of Art. 6(9) of the DMA. The article mandates the portability of data provided or generated by a user from a gatekeeper organisation to the end-user directly or a third party authorised by the end-user. This raises a number of questions regarding privacy and security with respect to the data in scope of the DMA obligations. We recommend solutions towards enabling the DMA's policy objectives without compromising privacy rights and obligations or the security of individuals.

For the data sharing obligations under the DMA to achieve their aim without potentially negatively impacting individuals and eroding trust in the digital ecosystem, the following will be necessary:

- Further guidance on the categories of data not subject to the data-sharing obligations, either because they do not support the aim of the DMA's data portability obligations of switching and multi-homing or are negatively impacting third-party rights;
- Clarifying how the GDPR legal bases for processing, especially Article 6(1)(c) GDPR, applies in the context of the DMA's mandatory data-sharing;
- Developing co-regulatory codes of conduct and data-sharing frameworks that include technical standards as well as minimum security standards for data recipients similar to existing examples such as open banking;
- Clarifying the role of the gatekeeper in conducting risk assessment and clarifying the factors and safeguards to be considered before engaging in data-sharing under the DMA.

1 CIPL is a global privacy and data policy think-and-do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website.

2 Centre for Information Policy Leadership, Bridging the DMA and the GDPR, 2022.

3 Centre for Information Policy Leadership, Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences, 2023.

I. Data Mobility Under the DMA

One of the DMA's objectives is to minimise the risk of lock-in effects for both individuals and organisations in the context of digital services and to facilitate the movement of data from gatekeeper platforms and services to third parties. The DMA has enacted a number of data-sharing obligations in business-to-business (B2B) and business-to-consumer (B2C) contexts specifically to ensure that switching and multi-homing are not restricted[4]:

> **Article 6(9) DMA**
>
> *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.*

> **Article 6(10) DMA**
>
> *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 for or 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 business users 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.*

These provisions raise some significant legal and technical implementation questions that are insufficiently or not at all addressed by the DMA or further relevant guidance from the European Commission.

4 Recital 59 DMA states: "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, end users, as well as third parties authorised by an end user, should be granted effective and immediate access to the data they provided or that was generated through their activity on the relevant core platform services of the gatekeeper."

1. Without prejudice to the GDPR

Data-sharing obligations will inevitably encompass personal data, particularly within the context of Article 6(9) DMA. This provision pertains to data initially provided by the end user, as well as data generated by the end user through the utilisation of the gatekeeper's core platform service. Given that personal data processing in the EU is governed by the GDPR, it raises additional questions regarding the interplay between the GDPR and the DMA.

The DMA is intended to apply without prejudice to the GDPR and is explicitly not *lex specialis* to the GDPR.[5] As a result, effective personal data protection, as a fundamental right, cannot be hampered by decisions made to improve contestability or fairness in the digital single market. Conversely, the GDPR should not be interpreted in a way that unnecessarily undermines effective competition and economic growth. Article 8(1) DMA specifically demands any obligations under Article 6 DMA to also be in compliance with GDPR. Against this background, the data mobility obligations of the DMA continue to raise a number of unanswered questions on the interaction of DMA and GDPR. [6]

2. Data Scope

To begin with, questions remain as to what data is in the scope of the data-sharing obligations under the DMA. Art. 6(9) DMA defines the scope of data to be made available as data provided directly by the user and *data generated by the end user through their activity on the core platform service*. Beyond the purpose for the portability obligations outlined in Recital 59, the DMA does not provide any further definition of what that might entail or how that data should be delimited.

The GDPR equally provides individuals with the right to the portability of data they provide in Art. 20. In that context, the EDPB defines *"provided"* as data the individual actively submitted (e.g. mailing address or user name) but also data "observed" from the activities of the user (the EDPB refers to search history or activity logs).[7] However, the full scope of "observed" data continues to be a topic of discussion.[8] The EDPB at least understands the data portability right of Art. 20 GDPR as a right to a subset of the personal data processed by a data controller to the exclusion of data created by the controller. [9]

The DMA uses the same terminology, and it would be reasonable to assume that the same interpretation of "provided" data would apply as with GDPR.[10] This would also be in keeping with the understanding concerning data to be shared in the Data Act. Recital 14 of the Data Act refers to data as the "digitisation of user action and events", essentially excluding derived or inferred data, which would be based on an action of the gatekeeper/controller. For a coherent implementation and the avoidance of fragmentation and legal uncertainty, a consistent approach to overlapping legal concepts in the DMA, DA, and GDPR is imperative.

Additionally, data portability under the DMA must be governed by considerations of proportionality and necessity and take into account the purpose of Articles 6(9) and 6(10) DMA, namely to facilitate, in accordance with Recital 59 DMA, switching and multi-homing ensuring contestability and innovation potential. The EDPB is clear that the GDPR is not regulating competition, and any effect of data portability under the GDPR on competition is incidental. [11] Conversely, the DMA makes it clear in Recital 59 that the data portability obligations under the DMA are specifically intended to enable switching and multi-homing f*or purposes of competition*. Consequently, data that is not necessary toward this goal, especially personal data, would not be within the scope of the data portability obligations of the DMA and should not have to be provided.

5 See also CIPL discussion paper "Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences", May 2023, p. 5.

6 See CIPL Paper Bridging the DMA and the GDPR - Comments by the Centre for Information Policy Leadership on the Data Protection Implications of the Draft Digital Markets Act.

7 WP 242 "Guidelines to Data Portability" as adopted by the EDPB.

8 See also Jan Krämer, "Data Access Provisions in the DMA", CERRE, November 2022, p. 7.

9 WP 29 "Guidelines to Data Portability" as adopted by the EDPB, p. 10.

10 This is also supported by Recital 59 DMA, which explicitly stipulates that the data portability obligation complements those of the GDPR.

11 WP 29 "Guidelines to Data Portability" as adopted by the EDPB, p. 4.

The European Commission should, therefore, provide clear guidance regarding data "generated through the activity of the end user in the context of the use of the relevant core platform service", clearly excluding categories such as inferred and derived data from scope.

Additionally, Art. 20(4) GDPR clarifies that the right to data portability may not adversely affect the rights and freedoms of others. This qualification is missing for the data portability obligations under the DMA. There are many examples in which data generated or observed may be linked to the personal data of other individuals, such as photos or videos containing multiple individuals, saved locations such as home addresses, interaction with content such as tags or comments, search queries containing personal and even sensitive data to name a few. The Commission will need to clarify further whether the same restriction as in the GDPR applies to the DMA data sharing obligations, by extension, where personal data of third parties is concerned.

Failure to adopt a coherent approach may bring legal uncertainty in the context of the implementation of data portability and possibly undermine its full potential. While data portability under the GDPR addressed to the individual continues to have limited practical adoption, the DMA re-invigorated the discussion, and it certainly would be the expectation that the DMA data sharing obligations, specifically to third parties, will enjoy much wider use, given requirements for ease of delivery, frequency, as well as the perceived commercial value of the data.[12]

12

II. Challenges to Operationalizing Data Sharing

To the extent personal data is shared under Art. 6(9) or 6(10) DMA, the entity sharing the data requires a legal basis in compliance with Art. 6 GDPR. The Commission, along with the EDPB, should clarify that the data-sharing obligations under the DMA fulfil the requirements of a legal obligation under Art. 6 (1)(c) of the GDPR for the sharing gatekeeper.

More importantly, the obligation to provide access to data, especially in a continuous and real-time manner, in the modern data infrastructure is complex and technically challenging to implement. Depending on the situation, continuous and real-time access also has the inherent potential to result in unintended harm to the end user, such as heightened risks of data misuse, privacy violations, or disclosure of otherwise sensitive data.

Data in the scope of Art. 6(9) and 6(10) DMA will inevitably involve a variety of data types: personal and non-personal, structured and non-structured, and different technical formats. It may also be very large in volume, which can pose bandwidth challenges and raises the question of whether an upper limit or technical feasibility defence parallel to Art. 20(2) GDPR should be considered.

Data export options do depend on the service but may ultimately mirror or supplement GDPR portability settings, possibly through an API portal with an authorisation mechanism and choices concerning[13]:

- Data categories
- Data volume
- Sharing frequency

Data in scope for the DMA's data portability obligations will not necessarily be located in one large data lake from which it could be distributed but in different systems and will likely exist in a variety of formats. It may have to be pooled before access can be provided, and some measure of verification must be performed to ensure the correct user data is being shared to avoid creating a data breach scenario to the detriment of user rights. This may mean that not all data is available instantaneously, and some degree of latency may be inevitable.

13 For example, Amazon provides data portability in two ways: by sharing data with an authorised third-party through an API and through a self-service download portal accessible by Amazon customers (Transfer Your Data portal); Amazon customers are able to select the specific data categories they wish to share with the third party, and Amazon alerts them to the potential risks and consequences of sharing their personal data with third parties. Finally, customers need to tick a box explicitly authorising a third party to receive the personal data selected by the customer before clicking "Authorize" (Amazon DMA Compliance Report, p. 9). Subsequently, the authorised third party can call the Portability API and receive data according to the customer's preferences. Similarly, other gatekeepers have also enabled data portability APIs: Google through a Data Portability API, LinkedIn through a Member Data Portability API, Apple through an Account Data Transfer API, TikTok through a Data Portability API, Meta through Download Your Information and Transfer Your Information tools (Meta DMA Compliance Report, p. 5).

In the B2B context of Art. 6(10) DMA, data may also have to be aggregated, which assumes processing prior to the "real-time and continuous access", for instance, to distinguish personal data in a case where the individual has not opted into the sharing of their data. This poses obvious and significant challenges to the *real-time* aspect of access and raises questions as to a standard for data mobility under DMA.

As opposed to data sharing in the payment services sector under PSD2, where the data sets to be accessed or shared pertain to one very specific sector and recipients are well known, data access under the DMA will be across many different sectors of varying sophistication and capabilities. The DMA imposes obligations only on gatekeepers but none on data recipients to ensure data access is possible and secure.[14]

14 The Directive 2015/2366 on Payment Services (PSD2) aims to modernise Europe's payment services for the benefit of consumers and businesses. The Directive has a limited scope as it only applies to payment services listed under Annex I of the Directive. It also imposes specific requirements on potential data recipients.

III. Obligations and Liabilities of Gatekeeper and Data Recipient

The GDPR imposes obligations on all actors to the extent they process personal data - the gatekeeper, the recipient of the data and other business partners. As such, compliance with the GDPR is a shared responsibility that requires thoughtful collaboration between organisations sharing data and organisations receiving data. Under the GDPR, data recipients would become new data controllers and, as such, be bound by the same processing limitation and obligations to safeguard the (personal) data received as the data sender, which was the original controller. The DMA, however, which incidentally has broader application than personal data alone, is focused solely on the obligations of the gatekeeper to share data with third parties on authorisation by the end user, even in real time. This raises a number of concerns that will need further consideration. [15]

1. Validity of Data Sharing Authorisation

The gatekeeper will have little visibility into the purpose for which the (personal) data to be shared will be used or why the user is consenting. There are several potential risks that should be considered in this regard:

- The authorisation portal must comply with Art. 6(9) and 6(10) DMA and will be provided on the gatekeeper side for the third party to link to; there is little visibility into whether the third-party recipient has a valid legal basis for processing the personal data of the user beyond the user authorisation, whether the request to provide access to the data was presented sufficiently clearly by the third party and in a way the end user can understand, or whether nudging techniques were deployed to incentivise consent in exchange for a new App or to participate in an online game without sufficient indication for the ultimate data use. It should be noted that the Data Act, on the other hand, makes it specifically clear in Recital 34 that the data recipient of data shared under the Data Act is not to use coercive or deceptive measures to influence the decision of the user to share their data.
- While authorisation for data sharing under the DMA is given through the gatekeeper interface and should also be withdrawn that way, the individual may not understand or remember this and instead contact the third party without also informing the gatekeeper.
- Users may ultimately not remember which third party they authorised for which data categories and for what purpose without some form of prompt.
- The volume or type of data authorised may go beyond what is necessary for the purpose of the recipient (or indeed the purpose of supporting multi-homing and switching), and the purpose may not be fully explained. The legislators seem to have considered such a scenario in Recital 33 of the Data Act, for example, which requires that *"third parties to whom data has been made available upon request of the user should only process the data for the purposes agreed with the user and share it with another third party only if this is necessary to provide the service requested by the user"*.
- Third-party data recipients may in some instances even be outside the scope of the GDPR entirely or in a jurisdiction that would make prompt enforcement by EU data protection authorities challenging.

15 See also Wojciech Wiewiórowski, "Sharing is caring? That depends...", 2019.

2. Data Security

A major unresolved concern raised by the data-sharing obligations of the DMA is data security. Malicious actors may exploit the possibilities of direct data transfers of user data to third parties under the DMA for nefarious purposes. The GDPR, in particular Art. 5(1)(f) and Art. 32 impose certain security standards on data controllers processing personal data in the Union, requiring *appropriate technical and organisational measures* and Art. 8 (1) DMA reminds gatekeepers to ensure that measures taken in compliance with Art. 6 DMA also comply with the GDPR. However, the same may not apply to the data recipient, who, in the case of business users outside of the EU jurisdiction, might not even always be subject to GDPR.[16] Although the DMA only allows gatekeepers limited measures to protect their own systems and enables end-users to do so in relation to third parties, there are no provisions for gatekeepers to conduct even basic due diligence on the data recipient. Considerations to not provide data on the basis of security concerns with respect to the third party would certainly have to be very carefully weighed, given the risk of non-compliance proceedings.

However, as experts have observed: "Refusing to exchange our data with unidentified, unvetted third parties is precisely what we should expect from digital service providers."[17] In particular since, the high level of data security gatekeeper organisations can provide may often mean "trading down" in terms of data security when exporting data. A data breach due to insufficient data security measures of the data recipient can have a devastating effect on the individual end-user and may also lead to a loss of trust in the gatekeeper and the digital economy more broadly. End users will not necessarily understand the complexities of the DMA obligations, such as where the security breakdown occurred and where liability is to be assigned.

Similarly, DPAs may initially commence data breach investigations against gatekeepers for security issues under the sole control of the data recipient, with gatekeepers having to expand further resources to exculpate themselves. Where the recipient of data under the DMA is located in a jurisdiction outside of the Union, it is likely that the end user and those who make it their business to represent them will inevitably attempt to seek redress from the gatekeeper. Given that the gatekeeper is obligated to share the data and depending on the technical set-up of the data exchange, liability for a cyber incident may not always be clear-cut.

It should, therefore, be considered to what extent third-party data recipients should fulfil sufficient security standards and to what degree the gatekeeper can verify the same in advance of any data transfers to the third party. Unlike in the context of PSD2 or Open Banking, there are no minimum standards at present to ensure the protection of the end-user data nor any accreditation bodies that might certify adherence to any standards. While Art. 6(10) DMA may see at least some of the issues discussed above addressed in B2B data sharing agreements, Art. 6(9) DMA presents a different scenario. There will likely not be any pre-existing (business) relationship that might set standards for the sharing of data, potentially leaving the individual (and the gatekeeper) exposed to bad actors.

Interestingly, the Data Act has considered the use of data received by a third-party recipient in Recital 35, requiring the third party to refrain from using the data to profile individuals, for instance. However, the DMA appears more focused on the gatekeeper.

While most gatekeepers have taken measures in their compliance solutions to ensure a basic level of security,[18] we note that Art. 48 DMA gives a mandate to the Commission to invite European standardisation bodies to develop standards in support of the DMA obligations. Existing ISO standards could equally be leveraged. A security standard for authorised third-party data recipients with corresponding certifications would allow the gatekeeper to verify sufficient protection of the transferred data. This would have to correspond with the possibility for the gatekeeper to refuse transfer, where the data recipient cannot show they are meeting the necessary requirements, or stop transfers, for instance, where the certification lapsed, or a significant data breach became known. A standard would be equally beneficial for third parties interacting with different gatekeepers – there would be one standardised verification process valid for all gatekeepers rather than a patchwork of approaches.

16 De Streel and Monti in CERRE "Data -Related Obligations in the DMA" insist that adherence to the GDPR by third-party recipients during and after the transfer is a key factor for the effectiveness of Article 6(9) portability obligations, p. 90.

17 Mikołaj Barczentewicz, "The Digital Markets Act is a security nightmare", 2022.

18 DMA Compliance Reports are available through the Commission's website.

IV. Recommendations

It is important that the DMA's provisions involving the sharing of personal data are not looked at in isolation and only from the gatekeeper's perspective. Data portability under the GDPR supports the request of an individual to receive their data and use it how they see fit, including sending it to third parties, and involves case-by-case assessments. The DMA, however, obliges gatekeepers to pursue sharing practices upfront and directly with third parties authorised by the end user without any standards or guarantees the data recipient is subject to data protection and security obligations to an equivalent level of the gatekeeper or adheres to them. This poses the inherent risk of adversely affecting individuals' rights and freedoms when bad actors exploit the data, or the third party does not have sufficient security measures to protect against data leaks.

Currently, there is no comprehensive guidance from the European Data Protection Board (EDPB), the European Commission or the national Data Protection Authorities (DPAs) to help organisations share, give access to, and receive data in compliance with the GDPR and the DMA. The UK's Information Commissioner (ICO) has published a Data Sharing Code of Practice that helps describe some of the practical consequences of data sharing and assists in the creation and implementation of the sharing frameworks in compliance with the GDPR. Similarly, in Singapore, the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) have created the Trusted Data Sharing Framework to help users understand key considerations to enable data sharing. There are also non-governmental efforts to create data portability standards, such as the Data Transfer Initiative. The European Commission should consider similar further guidance on data sharing in cooperation with members of the EDPB, for instance, when it comes to personal data.

Gatekeepers should be asked to evaluate the level of adverse impact through risk assessments before sharing data or providing access to data. Risk assessments have become ubiquitous since the GDPR and find application in the context of the implementation of emerging and new technologies, such as AI, but there still is no agreed risk framework or consensus on how to evaluate risks and harms. In the context of DMA data mobility, more work is certainly needed to understand the risks and harms that are inherent in the process and to identify proportionate mitigation measures. This will necessarily have to be an iterative multi-stakeholder process, including gatekeepers and regulators, as well as developers and data recipients.

For the data-sharing obligations under the DMA to achieve their aim without potentially negatively impacting individuals and eroding trust in the digital ecosystem, the following will be necessary:

Further guidance on the categories of data not subject to the data-sharing obligations either because they do not support the aim of the DMA or impact third-party rights;

- Clarify how the GDPR legal basis for processing, especially Article 6(1)(c) GDPR, applies in the context of the DMA's mandatory data-sharing
- Develop co-regulatory codes of conduct and data sharing framework that include technical standards as well as sufficient security standards for data recipients similar to open banking
- Clarify the role of the gatekeeper in conducting risk assessment and clarify the factors and safeguards to be considered before engaging in data-sharing under the DMA

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at

http://www.informationpolicycentre.com/.

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

24232.0424