Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

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

Discussion Paper | December 2021

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW

HUNTON ANDREWS KURTH

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

CIPL Recommendations

- Encourage and enable informed, cross-disciplinary, constructive regulatory dialogue and exchanges with experts and stakeholders on the interplay between DMA's obligations and the GDPR, both during the legislative process and the on-going implementation and development of the interpretation and guidance;
- Consider the interplay between the DMA's obligations and the GDPR, including data protection principles, data subjects' rights, and responsibilities of gatekeepers and data recipients;
- Build consensus on risk assessment, factors and safeguards to be considered by gatekeepers before engaging in data-sharing under DMA;
- Ascertain the categories of data not subject to the data-sharing obligations;
- Clarify the GDPR legal basis for processing for DMA's mandatory data-sharing, especially Article 6(1)(c) GDPR processing necessary for compliance with a legal obligation;
- Develop co-regulatory codes of conduct and data sharing frameworks;
- Encourage the voluntary release of useful, anonymised datasets and the overall data mobility within the EU;
- Provide incentives or endorsements to companies that practice data openness and responsible data sharing;
- Promote existing collaborative practices and tools, such as open data agreements, and facilitate cooperation among smaller digital players' data pooling practices;
- Encourage innovative regulatory tools, such as regulatory sandboxes and policy prototyping, including across the different regulators - data protection and competition;
- Develop EU Commission guidelines on the DMA's prohibitions and obligations through a process of regulatory dialogue to obtain stakeholders' views and expertise; and,
- Establish formalised cooperation between data protection and competition regulators to enable both a well-functioning data economy and effective data protection.

OBJECTIVES OF THE PAPER

The EU digital strategy intends to establish a safe and trusted digital space for individuals and a level playing field for businesses that fosters innovation, growth, and competitiveness in the EU.[1] Specifically, the draft Digital Markets Act (DMA)[2] aims to enable open and fair digital and data markets by fostering competition. In particular, it seeks to promote data mobility by imposing obligations on online platforms, falling under the category of "gatekeepers," to share or to provide access to data. The draft DMA also intends to strengthen the ability of business and end-users to utilise software applications on gatekeepers' core platforms without being confronted with technical restrictions. Mandatory data mobility is intended to reduce the risk of lock-in for individuals and organisations, offer business opportunities to a wider spectrum of market players and market entrants and enable individuals to move swiftly to new services and providers. Data mobility involves the sharing of data sets that may include personal data, hence triggering the application of the General Data Protection Regulation (GDPR).[3]

The objective of this paper is to:

a) Analyse the relationship between the DMA's data sharing obligations and the GDPR requirements;

b) Identify the areas that require further assessment and clarification; and

c) Inform and initiate necessary discussions on more practical aspects of the interplay between these two important legislative and policy pillars of the EU digital and data policy.

We expect that there will be a need for more work, constructive engagement and regulatory dialogue to find solutions that enable both competition and the protection of personal data and individuals' rights in the context of the DMA and the EU digital market.

[1] European Commission, Digital Services Act Package.
[2] European Commission, Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), 15 December 2020, COM (2020) 842 Final. This paper uses indistinctively the terms "DMA" or "draft DMA." Please also note that this paper is based on the analysis of the European Commission's original draft DMA proposal and will not analyse subsequent amendments proposed or adopted by the European Parliament or Council due to the incomplete legislative journey of the proposal.
[3] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data ("GDPR").

The Centre for Information Policy Leadership (CIPL)[4] has been at the forefront of promoting responsible use of data for more than 20 years. Building on our work on accountability and effective data protection,[5] in this paper CIPL analyses how the relevant DMA obligations involving personal data would interact with the GDPR. We also examine the operational consequences of the DMA obligations for gatekeepers and for the organisations receiving or getting access to personal data. Finally, we propose solutions to enable the achievement of the DMA's policy objectives in compliance with the GDPR and its dual aims to protect individuals' personal data and enable free flow of data within the EU.

The DMA states that it should complement the GDPR without prejudice to its application.[6] Yet, what this means in practice for organisations subject to both legal regimes is that it has not been explored in depth and remains rather obscure. As the relationship between competition law and data protection law keeps on evolving and is subject to much legal and policy analysis,[7] it is important that their interaction is considered on a case-by-case basis. No upfront determination should be made that one topic should systematically have priority over the other and that a competition risk analysis should prevail over any data protection risk analysis or vice-versa.[8] Effective personal data protection, as a fundamental right, cannot be hampered by decisions made to improve competition in the market. Conversely, narrowly construed interpretation of the GDPR cannot prevent effective competition and economic growth based on EU data and digital economy. The right to the protection of personal data is not an absolute right and must be considered in relation to other fundamental rights and its function in society.[9]

Further, the DMA's provisions involving the processing of personal data should not be looked at in isolation and only from the gatekeeper's perspective. The GDPR imposes obligations on all actors of the data supply chain and the data ecosystem - 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.

---

[4] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 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. CIPL generally develops its white papers and public consultation responses with input from its member companies. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[5] CIPL White Paper on "Organisational Accountability - Past, Present and Future", 30 October 2019; CIPL Paper on "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework" 27 May 2020.

[6] See Recital (11) of the DMA.

[7] Digital Crossroads: The Intersection of Competition Law and Data Privacy, Erika M. Douglas, 7 October 2021.

[8] The EU jurisprudence holds the view that any issues relating to the sensitivity of personal data are not, as such, a matter for competition law, but may be resolved on the basis of the relevant provisions governing data protection. See Case C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL and Administación del Estado Asociación de Usuarios de Servicios Bancarios (Ausbanc),* Judgment on 23 November 2006, para 63; Case M-4731, *Google/DoubleClick Regulation No. 139/2004 Merger Procedure,* 11 March 2008, para 368; Case M-7217, *Facebook/WhatsApp Regulation No. 139/2004 Merger Procedure,* 3 October 2014, para 164.

[9] See Recital (4) of the GDPR.

Finally, it is important that the DMA does not create legal uncertainty, open-ended liability, conflicts of laws and data protection risks that may affect an individual's trust and an organisation's readiness to engage in digital and data economy. An unclear legal framework without sufficient opportunity for regulatory dialogue and certainty could create some reticence from companies receiving the data to reuse it in innovative ways, which could also ultimately reduce competition.

1. Understanding the DMA's provisions involving the processing of personal data

The DMA contains several provisions that would impose obligations on the gatekeeper to share or to provide access to personal data (see Appendix 1, summary table of all relevant obligations in the draft DMA). Both the access to and the sharing of personal data constitutes processing of personal data subject to the GDPR.[10]

1.1 Wide spectrum of the obligations involving personal data

Some DMA provisions impose the obligation on gatekeepers to share or provide access to their data[11] to various recipients:

- To existing business partners (or "business users" in the DMA): Obligation for the gatekeeper to provide some of business partners an effective, high quality, continuous and real-time access and use of aggregated and non-aggregated data, that has been provided or generated in the context of the use of the gatekeeper's core platform services.

- To competitors: Obligation for the gatekeeper to provide fair, reasonable and non-discriminatory access to ranking, query, click and view data in relation to free and paid searches by end users to competitors;

- There may be additional scenarios in which the EU Commission may require gatekeepers to implement specific measures that may involve further obligations to share data or to render it accessible to competitors, other business partners or third parties.

[10] The definition of "processing" under Article 4(2) of the GDPR is broad and includes, "the disclosure by transmission, dissemination or otherwise making available of data;" see, also, the EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), 9 June 2021, para 32.

[11] Because the distinction between personal data and non-personal data is becoming increasingly complex (see Section 2.2), this paper refers indistinctively to the notions of data and personal data.

Some DMA provisions relate to promoting individual rights, control, choice of services and informational self-determination.[12] The provisions provide the following:

- An obligation for gatekeepers to provide tools to individuals (or "end-users" in the DMA or "data subjects" in the GDPR) to facilitate the exercise of data portability rights, including by the provision of continuous and real-time access to data. This obligation, aimed at increasing competition, also overlaps with and may facilitate the implementation of the access and data portability rights under GDPR.

- An obligation for gatekeepers to refrain from combining personal data sourced from their platform services with personal data from their other services, or with personal data from third-party services unless the end-user has consented.

- An obligation for gatekeepers to allow end-users to install and effectively use third-party software applications or software applications stored on operating systems of the gatekeeper.

CIPL notes that while straightforward in theory, the obligation to provide access to data in a continuous and real-time manner may be complex, far-reaching and technically hard to implement. In addition, depending on the situation, it could result in unintended harm to end user's rights and innovation (such as heightened risks of data misuse, privacy violations, or disclosure of trade secrets) without necessarily fostering contestability or fairness as envisioned in the DMA. In particular, in the absence of a regulatory dialogue with impacted stakeholders on the practical and technical implementation, the obligation to share data is likely to create challenges for gatekeepers for the following reasons:

a) it would apply to any type of data, including unstructured data or data stored in different systems for different purposes;
b) this obligation is not confined to a single sector, but would apply across different sectors and types of gatekeepers;
c) such data may also have to be made accessible to numerous recipients in different sectors;
d) it may cover data that does not necessarily create competitive advantage and, thus, the obligation to share that data would not further the purpose of the law.

This is quite a different fact pattern from the implementation of the PSD2 Directive in the financial sector, for example, where the data sets required to be made accessible are limited to one sector and the recipients are well identified, too.[13]

[12] This paper focuses on data sharing provisions of the DMA and their interactions with GDPR. CIPL will analyze the privacy and security implications of DMA's other key obligations, such as sideloading practice in relation to technical restrictions, in a separate op-ed following the publication of this paper.

[13] The Directive 2015/2366 on Payment Services (PSD 2) 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. Finally, data sharing activities under open banking have been challenged from a trust perspective because new entrants into the system may err on the side of making authentication too easy or too difficult, which either affect customer security and privacy, or consumer experience. See HID White Paper on Opportunities and Challenges of Open Banking Around the World, 20 February 2020, page 4.

1.2 Reference to the GDPR taxonomy

The DMA takes into account the fact that some of the obligations of the gatekeeper to share or provide access to data relates to personal data and imposes additional obligations that are inspired by the terminology of the GDPR. These may include:

- An obligation that any measures implemented to comply with the DMA's gatekeepers' obligations comply with the GDPR and ePrivacy Directive;

- An obligation to anonymise personal data in some specific instances;

- An obligation to provide access to and use of personal data, that is directly connected with the use of the business users' products or services by the end user and when the end user gives GDPR consent;

- A prohibition to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of the GDPR;

- An obligation for the gatekeeper to enable business users to directly obtain the consent required for their processing, where data subject consent is required to ensure compliance with the DMA, or to comply with data protection law in other ways, such as by providing anonymous data where appropriate. This includes obligations not to make it more difficult for business users to obtain consent than it is for the gatekeeper.

Some of the DMA's obligations make an explicit reference to the need for the gatekeeper to comply with the GDPR. Others require that the individual provide consent before data can be shared and some require the gatekeeper to facilitate compliance by business users and, some others remain silent. Thus, the EU Commission and the relevant regulators should encourage and enable informed and cross-disciplinary discussions and constructive regulatory dialogue and exchanges with experts and stakeholders on the interplay between DMA's obligations and the GDPR, both during the legislative process and the on-going implementation and development of the interpretation and guidance.

1.3 Learning from other regulations involving data sharing

Currently, there is no available guidance from the European Data Protection Board (EDPB) nor the national Data Protection Authorities (DPAs) to help organisations share, give access and receive data in compliance with the GDPR. Albeit, not any more a member of the EU, only the UK's Information Commissioner (ICO) has published a Data Sharing Code of Practice[14] that helps describe some of the practical consequences of data sharing and assists the creation and implementation of the sharing frameworks in compliance with the GDPR.

In addition, some useful lessons can be learned from the implementation of the individuals' data portability right under the GDPR.[15] Both the GDPR and the DMA are intended to improve data mobility and choice in services for end users in a mandatory manner. In the context of GDPR data portability provisions, the sharing entity (controller) is acting pursuant to the request of an individual exercising his/her right. In the context of the DMA, the sharing entity (gatekeeper) would be acting pursuant to a legal obligation or an EU Commission decision. Data portability under the GDPR poses similar types of operational challenges as the obligation to share data under the DMA. For example, the availability of a standard technical framework and clarity on the respective obligations and liabilities of the sharing and receiving entities are pre-conditions for effective data portability. That said, the extent and complexity of these operational challenges for the DMA obligation far exceed those for the GDPR. This is because while data portability under the GDPR enables data sharing of a single individual for that individual's use case, the DMA obligation on gatekeepers to share data may cover entire datasets relating to a large number of individuals and covering different datasets and processing activities by a large number of third party businesses who seek to use those datasets for a range of commercial purposes.

Finally, there are some parallels with the EU Data Strategy,[16] which aim to create a data governance framework to facilitate data sharing across organisations, sectors and Member States. This strategy is reflected in the Data Governance Act (DGA)[17] and the upcoming Data Act. The DGA is setting up the structure to promote the free flow of data and enhanced data mobility and sharing in the EU and, in particular, data held by the public sector. Public sector bodies allowing the re-use of data under DGA would need to ensure the protection of personal data, just like the gatekeepers under the DMA. The upcoming Data Act will foster data sharing between organisations and will also require compliance with the GDPR.

While the DMA aims to be complementary with the GDPR without prejudicing its application (Recital 11 DMA), organisations can only achieve compliance with that objective through careful consideration and further engagement and guidance by relevant regulators. Without regulatory or legislative clarification, gatekeepers may find it challenging to deliver both compliance with some of the DMA's data sharing obligations and the GDPR. This is especially the case in the absence of any guardrails or safeguards

[14] Information Commissioner's Office, ICO Publishes New Data Sharing Code of Practice, 17 December 2020.
[15] See Article 20 of the GDPR; see Article 29 Working Party Guidelines on the right to "data portability" adopted on 13 December 2016 as last revised and adopted on 5 April 2017. See CIPL Response to the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" February 15, 2017.
[16] European Commission, European Data Strategy.
[17] Proposal for A Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), 25 November 2020; and EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), 9 June 2021.

provided by the law or the regulator (whether the data protection regulators or the competition regulators), and where data must be shared or made available to a high number of recipients for an unlimited timeframe.

2. Implementing the DMA's obligations involving the processing of personal data

The DMA provides that the gatekeeper shall comply with the GDPR when executing its obligations. This calls for careful consideration and will require both gatekeepers and business users to address necessity and proportionality, legal basis, purpose limitation and data subject rights, as underlined by the European Data Protection Supervisor (EDPS).[18] Complying with the GDPR is not a "one-off" or an isolated action. It concerns both the gatekeeper sharing the data and the recipient reusing such data. The recipient of the data is not given a "carte blanche" to reuse the data, but would have to comply with all the provisions of the GDPR.

Below we outline the main provisions of the GDPR that will have to be considered and complied with by all the stakeholders in any data sharing initiative.

2.1 Identifying the roles of the stakeholders and the data in scope of the data sharing obligation

As any organisation subject to the GDPR, the gatekeeper may be acting as a **controller, a processor or joint controller** in relation to the data processed. These roles may have different consequences on the extent to and the conditions under which the gatekeeper will be able to share data as required by the DMA.

(a) **The controller** is the organisation which defines the purposes and the means of processing personal data.[19] As such, the controller is responsible for establishing the legal basis for processing of personal data (see section 2.3) and should be able, once the correct legal basis is identified, to share the data as requested under the DMA (subject, of course, to compliance with its other GDPR obligations);

(b) **The processor** is the organisation which processes personal data on behalf of the controller.[20] The relationship between the controller and its processor is defined by contractual terms in accordance with Article 28 GDPR. In particular, the processor can only process personal data on the instructions of the controller, unless required to process data by Union or Member State Law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing. It is unclear in this situation whether the DMA's data sharing obligations could also apply to the data processed by the gatekeeper as a processor and in particular whether the DMA's obligations would fall under the "Union or Member State law" exception (including when an EU Commission decision mandates the sharing of personal data that the gatekeeper processes on the instructions of a controller);

[18] See Sharing is caring? That depends…, European Data Protection Supervisor Blog, Wojciech Wiewiórowski, 13 December 2019.
[19] See Article 4(7) of the GDPR.
[20] See Article 4(8) of the GDPR.

(c) **The joint controller** is the organisation which defines jointly with other controllers the purposes and the means of processing personal data.[21] The relationship of the joint controllers is defined by a contract as per Article 26 GDPR that determines their respective obligations, in particular with regard to the exercising of the rights of individuals. In case the gatekeeper is acting as a joint controller for the data it must share under the DMA, it is unclear how this will affect the existing contract between the joint controllers and what the liabilities will be to each of them and to one another, as well as to the individuals.

Another important question arises as to the **determination of the data in scope of the sharing**. The different provisions of the DMA are inconsistent in this respect - some require "access to data," others require access to "data that is provided for or generated in the context of…" or "access to data in relation to…." Failure to adopt a more coherent approach may bring the same legal uncertainty as in the context of the implementation of data portability requests under Article 20 of the GDPR.[22] Under the GDPR, data portability right is limited to data provided by individuals, yet in its guidance the EDPB has extended the interpretation of the right to cover inferred and observed data. Should the provisions of the DMA also be confined to data provided by individuals or extend to data observed, data inferred, data created through routine user interaction, and if so, in which circumstances?[23] CIPL believes that it is important that the DMA (a) clearly define the scope of data that is subject to the data sharing obligations, also limiting it to the data necessary to enable competition, and (b) allow for regulatory dialogue to implement the DMA in ways that are consistent with other applicable laws, such as privacy and IP laws (for instance, in relation to commercially sensitive trade information or proprietary algorithms). It is important to take a balanced approach and ascertain the potential impact of any data sharing requirements on such data categories, so that the DMA's data-sharing and innovation-boosting objectives are not undermined. Lastly, data that is easily replicable or that has little competitive value in the core platform services should not be in the scope of the DMA, as it cannot reasonably be considered to restrict innovation.[24]

Another challenge relates to dealing with data sets that implicate privacy and data protection rights of

[21] See Article 4(7) of the GDPR. In *Wirtschaftsakademise,* the CJEU takes into account the fundamental role of the controller within the data protection system as accountable for data protection compliance. Therefore, the CJEU interprets the concept on a factual rather than a formal analysis and provides a broad interpretation in order to ensure the effective and complete protection for data subjects. Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein*, judgment on 5 June 2018, paras 27-28. Also, in *Fashion ID,* the CJEU solidified the broad definition of joint controllership, by holding an administrator of a fan page hosted on Facebook as a joint controller. Case C-40/17, *Fashion ID GmbH v Verbraucherzenrale NRW* eV, judgment on 29 July 2019, paras 65-70.

[22] The Working Party 29 and the EU Commission have reached different positions on the data in the scope of data portability requests under the GDPR. See Article 29 Working Party, Guidelines on the Right to Data Portability, 16 EN WP 242, Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017; European Commission, Experts Uneasy Over WP29 Data Portability Interpretation, David Meyer, 25 April 2017.

[23] Competition Policy for the Digital Era, Jacques Cremer, Yves-Alexandre de Montjoye, Heike Schweitzer, European Commission, 2019, pages 8-13. The report highlights the heterogeneity of data and its uses along many dimensions. Data can be categorised as volunteered, observed, or inferred data. It can be collected and used in different forms (individual-level data, device data, anonymous data, aggregated-level data). It can be generated at different frequencies and data access can either concern historical or real-time data.

[24] Ensuring Innovation Through Participative Antitrust, Oliver J. Bethell, Gavin N. Baird and Alexander M. Walksman, Journal of Antitrust Enforcement, March 2020, page 11.

more than one individual user, which is often the case for many consumer-facing digital platforms. In the context of a data portability request under the GDPR, Article 20(4) clearly provides that this right shall not adversely affect the rights and freedoms of others where, within a set of personal data, more than one individual is concerned. Should a similar provision also exist in the DMA and what its legal consequences would be for the gatekeeper, the recipients of the data and the individuals? For example, a transaction between two parties in the context of mobility pick-up/drop-off location and router details inherently relates to both a driver and a passenger. Nevertheless, it is important to note that data portability under the GDPR is triggered upon the request of data subjects and involves case-by-case assessments, whereas the DMA obliges gatekeepers to pursue the sharing practice upfront. Therefore, arguably, it would be more likely for sharing datasets to adversely affect third parties' rights and freedoms, especially considering the advanced re-identification techniques. However, gatekeepers could evaluate the level of adverse impact by performing risk assessment analysis in advance to identify the risks (including likelihood and severity) of sharing data or providing access to data. Risk assessments have become more commonly used with the enactment of GDPR and also in the context of implementation of emerging and new technologies, such as AI for example. Yet, there still is not an agreed risk framework, nor consensus on how to evaluate risks and harms. Hence, there will be a need for regulatory dialogue and guidance to determine the risk assessment factors and safeguards to be considered before sharing more comprehensive datasets.

2.2 Sharing of personal and non-personal data

Personal data and anonymised data – Experience with GDPR implementation shows that anonymising data according to the high standards of the GDPR may be difficult in practice. In addition, what is considered truly anonymised at a given point in time on the basis of certain state of the art technology, might not remain anonymised in the medium/long run. This is due to the possibility to re-identify personal data from a combination of non-personal data, in particular where such non-personal data includes anonymised personal data. In their opinion on the DGA, the EDPB/EDPS note that the risk of re-identification increases with the volume of non-personal data that is combined with other information.[25] Similarly, data scientists have shown that anonymising individual-level personal data in such a way that individuals cannot be re-identified is very difficult.[26] The more information there is, the more difficult it is to ensure anonymisation. In fact, this risk materialised in 2006 in the AOL search data leak when the company released twenty million search keywords of over 650,000 users over a 3-month period to the public in a non-identifiable (pseudonymised) format. As personal data was included in many of the queries, some users were identified by their search queries.[27] As a consequence, the DMA requirement for the gatekeeper to provide access to ranking, query, click and view data in relation to free and paid

[25] See Note [10], para 58. Also, see Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models, Luc Rocher, Julien M. Hendrickx, Yves-Alexandre de Montjoye, Nature, 23 July 2019, page 2.
[26] See Note [23], Competition Policy for the Digital Era, page 77. "Anonymous data do not contain any direct identifiers (such as name, address, email, phone number). However, a hacker trying to re-identify an individual in the dataset can use information (e.g., birth date and zip code) he has about the person, e.g., from publicly or easily available data, to re-identify him or her. While anonymising small data is hard, it is impossible for rich "observed" datasets using traditional statistical disclosure methods. For instance, such datasets containing location data from mobile phone, credit card transactions, smartcard tap-in tap-out, and browsing (URLs) datasets have all been shown to be re-identifiable."
[27] A Face Is Exposed for AOL Searcher No. 4417749, Michael Barbaro and Tom Zeller Jr., *The New York Times*, 9 August 2006.

searches by end users should be weighed carefully to ensure that this does not lead to possible re-identification of the shared data, in violation of individuals' data protection's rights. In its opinion on the DMA,[28] the EDPS highlights that the query, click and view data in relation to searches generated by individuals constitute personal data and, in some instances, sensitive data. Consequently, the impact of a re-identification on individuals can be very high. While the EDPS suggests that the gatekeepers should test the risk of re-identification before releasing the data, some studies conclude that "even heavily sampled anonymised datasets are unlikely to satisfy the modern standards for anonymisation set forth by GDPR."[29] This creates legal uncertainty both for the gatekeeper and the organisation receiving the data. This challenge is further amplified by the lack of consistent approaches among the EU DPAs on the best and acceptable way to achieve anonymisation, taking into account a risk-based approach.[30]

Personal data and aggregated data - The DMA imposes an obligation on gatekeepers to share both aggregated and non-aggregated data. These concepts are not defined under the GDPR. In its opinion on the DMA, the EDPS highlights that this wording may cause inconsistency with the GDPR. Both aggregated and non-aggregated data might in practice include personal data, yet the DMA implies that aggregated data is not personal data.[31]

Mixed data sets - Personal data is often combined or inextricably mixed with non-personal data. As the EU Commission noted "[m]ixed datasets represent the majority of datasets used in the data economy and are common because of technological developments such as the Internet of Things (i.e., digitally connecting objects), artificial intelligence and technologies enabling big data analytics."[32] The EDPB and the EDPS recall that as per the Regulation on the free flow of non-personal data, a mixed dataset is subject to all the obligations of the GDPR.[33] This means that gatekeepers are likely to be subject to the GDPR in the vast majority of cases where they have to share mixed datasets under the DMA.

2.3 Identifying the correct legal basis

In the context of the DGA, the EDPB/EDPS states that any provision of the DGA to share data or to request permission to process data do not replace the necessity to have a legal ground to process the data under the GDPR.[34] In the absence of a specific guidance, it is possible that they would apply the same reasoning in the context of the DMA, as the GDPR does not distinguish between voluntary or mandatory data

[28] See EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, 10 February 2021, para 32.
[29] See Note [25], page 2.
[30] See Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, 2 September 2021, pages 19 to 25 summarizing the diverging views of the DPAs on whether a lossy hashing procedure enables proper data anonymisation.
Also see, statement by the Dutch DPA that anonymisation of mobile phone location is not possible. Autoriteit Persoonsgegevens, Gebruik Telecomdata Tegen Corona Kan Alleen Met Wet, 1 April 2020.
[31] See Recitals 43 and 56 of the draft DMA.
[32] See Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on an Framework for the Free Flow of Non-personal Data in the European Union, 29 May 2019, pages 8-10.
[33] See Article 2(2) of the Regulation on the free flow of non-personal data: "*In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.*" Also see Note [10], para 61.
[34] See Note [10], paras 47-49.

sharing. In other words, DPAs may not interpret the DMA as creating the actual legal basis or replacing the need to have a legal basis for processing of data under the GDPR. Hence, gatekeepers will have to identify a correct legal basis before sharing data or giving access to data under the DMA.

Consent - Article 6(1)(a) GDPR - Some DMA provisions require that gatekeepers seek the consent of the individual end user under the GDPR to legitimise the sharing (including combination) of personal data with business users. These provisions limit the available legal grounds for such sharing to consent and are not consistent with Article 6 of the GDPR which includes multiple legal bases and puts them all, including consent, on an equal footing. CIPL strongly recommends that the interaction with the GDPR is fully considered when the DMA refers to GDPR concepts.[35] In addition and importantly, in the context of the DGA, the EDPB/EDPS question whether consent would be the appropriate legal ground in view of the individuals' ability to refuse to consent to the re-use of data, or to withdraw it at any time.[36] The same question arises in the context of the DMA. Subjecting the DMA's policy objective to open the data market to individuals consenting to data sharing, which includes the ability to withdraw such consent once data has been shared, would hinder the DMA's objectives. Also, it is very likely that this would trigger consent fatigue from individuals, as under the GDPR, individuals would have to actively opt-in to make such consent valid.[37] The withdrawal of end user consent across multiple platforms and businesses would also be technically challenging to manage and implement in practice, as the gatekeepers would have to cascade it to all recipients that may already have further processed the data. Also, the liability of the parties remains unclear in the case where it may not be possible to ensure that the actors in the data chain comply with the withdrawal of consent to share data, which inject further uncertainties around how the gatekeeper platforms and data recipients conduct their businesses under the DMA. Finally, any requirement to rely on consent must be carefully balanced with the objectives of the DMA to enable more and better mobility of and accessibility to data.[38]

Compliance with a legal obligation Article 6(1)(c) GDPR – This legal basis would be more workable in practice and more stable than the consent legal basis. It may also be more appropriate in light of the policy objective and provided specificity of the DMA, that would enable gatekeepers to confidently justify their data sharing obligations. Recital 45 of the GDPR provides that such legal obligation should have a basis in Union (or Member State) law. This law should determine the purpose of processing and specify the general conditions governing the lawfulness of the processing. The law should also establish specifications for determining the controller, the type of personal data processed, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and

[35] CIPL's Response to the EU Commission Consultation on the Evaluation of the GDPR, 28 April 2020, page 18.
[36] See Note [10], para 99.
[37] In addition, the recipient of the data may have to get individual consent to reuse the data for a specific purpose. It is unlikely that in case the gatekeeper has relied on the consent legal basis to share the data, it will be specific enough to cover also the subsequent processing activities of the recipient of the data.
[38] For instance, Article 5(a) of the proposed DMA prevents the combination of personal data from other services offered by the same platform unless end users have been presented with the specific choice and provided their consent. Lawmakers should consider the potential detrimental impact on the DMA's core objective of data sharing of frequent requests for consent for specific and narrow purposes as this may result in the failure by individuals to consent merely on the basis of consent fatigue rather than any substantive objections. Further, lawmakers might consider how any consent requirements might be designed to cover a broader range of purposes to reduce the frequency of consent request.

other measures to ensure lawful and fair processing. At this stage, the DMA does not provide nor can it realistically provide for all this detailed and context-specific information, and the question remains whether it could, at best, specify the types of data and recipients. There is little guidance at this stage from DPAs and the EDPB on this legal basis for processing. There is also an academic debate on whether a Commission decision can be considered as "required by law," in the same way as a law, regulation or any other statutory instrument.[39] It may be helpful to note that in its Data Sharing Code of Conduct, for example, the UK ICO clarifies that where data sharing is required by law, there is no need for the controller to seek individuals' consent for the sharing if the law clearly specifies that the sharing can take place without consent. It also clarifies that individuals have no right to object to the processing, as the data sharing is mandated by a legal obligation.[40]

Legitimate Interest Article 6(1)(f) GDPR - The legitimate interest legal basis requires a balancing of the legitimate interest of the controller or a third party (including society at large) against the fundamental rights and freedoms of individuals whose data is being shared. It also provides individuals with a right to object to the processing in case of overriding interests, although this right is not an absolute right.[41] This legal basis may be relevant in the context of the DMA and provide a valid legal basis for the entity sharing the data, as well as the entity receiving and processing the data. In order to promote consistency and facilitate the balancing test required by controllers under Article 6(1)(f), further dialogue with industry and guidance from EDPB on the application of legitimate interest in the context of DMA would be most helpful.

2.4 Complying with the data protection principles of Article 5 GDPR

All processing of personal data, including in the context of DMA, must comply with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability as per Article 5 of the GDPR.[42]

Transparency - Article 5(1)(a) and Article 13 and 14 of the GDPR require that individuals receive information about the use and processing of their personal data when data is collected directly from individuals and when data is obtained from other sources. In their opinion on the DGA, the EDPB/ EDPS underline that each actor of the data processing chain must provide individuals with transparent information. It recommends that this information be provided through user-friendly tools showing individuals a comprehensive view of how their personal data is shared. In the context of the DMA, this will require organisations to adapt their privacy notices to include that, in the case where they fall under

[39] Some commentators consider that this legal basis would require a generally applicable law rather than a specific decision or order. See Monopolisation Remedies and Data Privacy, Erika Douglas, *Virginia Journal of Law and Technology*, 25 November 2020, pages 84-85.
[40] See https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-c-case-studies/.
[41] CIPL White Paper on How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation, July 2021. For instance, organisations are subject to a multitude of laws and regulations, from reporting obligations to regulators, to law enforcement and judicial requests within the EU and abroad. Organisations often rely on the legitimate interests basis to share personal data when responding to these mandatory requests as reliance on the "compliance with a legal obligation" legal basis is not always possible. See page 18.
[42] See Note [10], para 73.

the definition of gatekeepers,[43] they may have to share data with some recipients, without being able to specify in most cases the type of data they would have to share,to which type of recipient, and for which use cases.[44] This would most likely require additional information to be provided to individuals at the time of actual data sharing. Equally, business users, as recipients of data, would have to provide separate notices to individuals about their own data use and processing practices. It is currently unclear what kind of infrastructure may be needed, and provide transparency about data sharing activities across the multiple platforms and businesses under the DMA. It remains to be seen how gatekeepers and business users can comply with this obligation, without increasing administrative burdens for themselves and over-burdening individuals with repeated notices for multiple data sharing. On the other hand, lack of proper transparency may also lead to a breach of the **fairness** principle, which is fundamental to the data sharing approach, according to the UK ICO.[45]

Purpose limitation - Article 5(1)(b) GDPR requires that controllers process data for "specified, explicit and legitimate purposes" and not use it in a way that is incompatible with the original purpose. Under the DMA, both the gatekeeper and the recipient have to comply with this principle. The gatekeepers would need to demonstrate that the data sharing is not incompatible with the original purpose, which may be challenging in most cases.[46] The recipient can process the data for many different purposes, such as to provide complementary services to a product or service provided by the gatekeeper in the same market or in aftermarket, or to train algorithms including for uses that are unrelated to activity of the gatekeeper,[47] or even for unrelated and new purposes. Hence, the recipient may find it challenging to ensure compliance with the purpose specification and limitation principles. In any case, the recipients will also need to ensure appropriate legal basis for their processing activities.

Data minimisation – In line with the GDPR overarching proportionality principle, Article 5(1)(c) GDPR requires that data be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. It is unclear how gatekeepers should comply with this principle when sharing data under the DMA. Should they share all the data as required by the DMA or any Commission decision even if they consider that this would not be compliant with the proportionality and minimisation principles or should they first assess how the data should be minimised? Some of the DMA's provisions indicate that the latter should apply.[48] However, there is a possibility that data that may be considered as strategic or relevant to some of the recipients may be removed, anonymised or pseudonymised by the gatekeeper who may prefer to focus on compliance with the GDPR rather than large data availability. This tension between obligations under the GDPR to ensure that the minimum amount of data is provided and the

[43] That determination will likely be not "carved in stone" as it will depend on the number of users and the company's turnover.
[44] See Article 13(1)(e) GDPR.
[45] Information Commissioner's Office, Fairness and Transparency in Data Sharing.
[46] The gatekeeper will not in most cases be able to ensure that the sharing of the personal data is compatible with the original purpose for which the data was collected as the gatekeeper won't collect the data for the purpose of sharing it with the third party. There would be three ways around this limitation: (a) obtaining the data subject's consent to "remedy" the purpose limitation issue; (b) each time data is being shared, carrying out a compatibility assessment under Art. 6(4) GDPR; or (c) the DMA -- as the legal basis for sharing the data -- could have an exception for the purpose limitation principle (see Art. 6(3) GDPR).
[47] See Note [23], Competition Policy for the Digital Era, page 13.
[48] See DMA articles requiring data minimisation practice from gatekeepers: Articles 5(1)(a), 6(1)(a), 6(1)(c), 6(1)(f), 6(1)(h), 6(1)(i), 6(1)(j), 6(1)(k), and Article 7(1) of the DMA (read in conjunction with the GDPR).

obligations under the DMA to provide sufficient information to third parties needs must be carefully considered and addressed. In addition, it is not clear at this stage which regulator (data protection of competition) should be the arbiter of this trade-off and how they may work together to come with a win-win solution.

Accountability principle - Article 5(2) of the GDPR requires organisations to put in place and be able to demonstrate risk-based policies and procedures to comply with the GDPR. Specifically, in the context of data sharing, it requires organisations to consider the risks that data sharing may create, and implement the appropriate mitigating actions. As part of the demonstration of compliance, organisations are required to maintain the relevant documentation such as a register of processing activities, risk assessments and DPIAs.[49] Accountability also requires organisations to demonstrate that they put in place policies and procedures that allow data subjects to easily exercise their rights and to document the data sharing decisions, including the purposes for which the personal data is shared and the recipients to whom data is disclosed.[50] The accountability principle is the cornerstone of effective data protection[51] and has to be implemented throughout the entire data chain, including the gatekeepers and all data recipients. Accountability is likely going to require that both gatekeepers and recipients develop a data sharing framework, with specific controls, policies and procedures. Again, development of such acceptable frameworks may benefit from a broader regulatory dialogue and engagement to ensure all the expectations are met and considered fully.

2.5 Privacy-by-Design

Article 25 of the GDPR provides that the controller shall implement appropriate technical and organisational measures to implement the data protection principles in an effective manner. Article 25(2) emphasises that this principle applies to the accessibility to personal data. The controller needs to ensure in particular that "by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." In addition, the EDPB Guidelines on the principle of privacy by design[52] include the requirements to refrain from further processing for new, incompatible purposes, as well as to limit the reuse of data. As a consequence, the DMA's obligations requiring the gatekeeper to share data with a potentially indefinite number of recipients may create uncertainty as to how this relates to this GDPR principle. The EDPS also acknowledges the tension between maintaining data's usefulness and lowering the risk of re-identification.[53] In the context of the DMA proposal, embracing a design facilitating data sharing obligation to foster competition objectives may inherently increase the risk of re-identification. Privacy Enhancing Technologies (PETs) may help to address this conflict in the future, when they can deliver proper anonymisation that does not reduce data availability, utility and relevance for the data recipients.

[49] See Note [14].
[50] See Note [10], para 138.
[51] See Note [5].
[52] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020.
[53] AEPD-EDPS Joint Paper on 10 Misunderstandings Related to Anonymisation, 27 April 2021.

2.6 Data Protection Impact Assessment (DPIA)

Article 35 of the GDPR requires that controllers perform a DPIA where processing is likely to result in a high risk to the rights and freedoms of individuals. The DPIA is intended to assess the impact of the processing on the rights and freedoms of individuals and to identify the relevant mitigation measures to address potential risks. Article 35(3) identifies circumstances where a DPIA is required and the EDPB and the DPAs have adopted specific lists of scenarios mandating a DPIA. In their opinion on the DGA, the EDPB/EDPS consider that a DPIA is a key tool to ensure data protection is effectively taken into account to foster individuals' trust in a "re-use mechanism." They recommend to include a provision in the DGA that sharing entities have to perform a DPIA in case the processing falls under Article 35 of the GDPR.[54] Similarly, the UK ICO recommends that the sharing entity perform a DPIA, even if not strictly legally required by the UK GDPR.[55] The DMA does not clarify whether gatekeepers would have to conduct a DPIA and whether they should identify the relevant mitigating measures to address the risk of sharing data or providing access to data. In many instances, such processing will trigger the GDPR and EDPB/DPAs thresholds requiring a DPIA. The gatekeeper may have to share data on a large scale or special categories of data or data relating to vulnerable persons (and even more so in the case of mandatory sharing of ranking, query, click and view data in relation to free and paid searches by end users on search engines of the gatekeeper). It is also unclear whether such DPIA should be made available to the recipients of the data and whether they would equally have to perform their own DPIAs for their processing made with the received data and/or comply with the mitigation measures included by gatekeeper in the DPIA.[56]

2.7 Security and due diligence[57]

Article 32 of the GDPR requires that organisations implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The GDPR recognises that effective data protection and security are joint responsibilities of organisations that are each responsible for the protection and security of the data. The obligation to ensure a sufficient level of security remains fully applicable in the context of the DMA. In order to enable effective data portability under the GDPR, several organisations have launched a data transfer project to build a common framework that can connect online service providers to enable seamless portability of data between two platforms.[58] The project is based on the assumption that each organisation is responsible for securing and protecting the data stored on its platform, regardless of whether it is supporting a transfer out, or receiving a transfer from another organisation. The project also allocates tasks and responsibilities between the individual exercising his/her right,[59] the data sharing entity and the receiving entity to ensure strong privacy and security to guard against unauthorised access to data (see summary table on allocation of responsibilities in Appendix 2).

---

[54] See Note [10], para 88.
[55] Information Commissioner's Office, Data Sharing Code of Practice: Deciding to Share Data.
[56] See Note [10], para 88. Where the entity sharing the data is a public entity, the decision on the re-use of data is based on the DPIA and on the specific conditions for the re-users and the concrete safeguards for individuals (for example, clarifying the risks of re-identification of anonymised data and the safeguards against those risks).
[57] See Note [12].
[58] The Data Transfer Project is an open-source collaboration supported by Apple, Deezer, Facebook, Google, Mastodon, Microsoft, Solid, and Twitter committed to building a common framework with open-source code that can connect any two online service providers.
[59] In the context of the DMA, the request to share data would not be initiated by an individual but would stem from a legal obligation or decision of the EU Commission.

Similarly, the Article 29 Working Party's guidelines on portability[60] highlight that the controller remains responsible for "taking all the security measures needed to ensure that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures)." The guidelines provide examples of risk mitigation measures, such as using additional authentication information, or suspending or freezing transmission if there is suspicion that an account has been compromised.

This raises a number of points that have to be clarified and further determined in the context of DMA:

a) To the extent that the data in scope contains personal data, how obligations to implement appropriate security measures would be transposed to the DMA and whether the gatekeeper should prioritise uncompromised security over compliance with the DMA (i.e., not being in a position to share the data with the recipient company(ies) if the security cannot be guaranteed);

b) Whether the gatekeeper would need to perform a security due diligence before sharing data with a recipient and what would be the consequences, if the gatekeeper were to conclude that the recipient does not offer a sufficient level of security. Sharing such data could put the gatekeeper in breach of its own data protection obligation. This question may be particularly relevant when the recipient of data is an SME that may not have the technical and security infrastructure to receive and protect the data efficiently;

c) Whether the gatekeeper should follow its own security standard or rely on recognised certifications to assess the level of security of the recipient and whether this would release the gatekeeper from any subsequent liability on the use of data; and

d) Whether the gatekeeper would have to monitor the data recipient's compliance with its security obligations as well as possible use restrictions attached to the data after the data has been shared.[61] Would the gatekeeper be also expected to enforce any non-compliance by the data recipient and/or inform the data protection regulator? How far do the gatekeeper's data protection obligations extend and to what extent they interfere with the DMA's policy objectives?

The UK ICO considers that the data sharing entity needs to take reasonable steps to ensure that the data shared will continue to be protected with adequate security by the recipient organisation. This includes ensuring that the recipient understands the nature and sensitivity of the data, or taking reasonable steps to verify that security measures are in place. The ICO considers that the sharing entity should also resolve issues before sharing data in cases where the recipient has different standards of security. [62]

2.8 Data sharing agreement

Organisations sharing and receiving personal data will most likely choose to define their respective rights and obligations in a legally binding instrument. The ICO also considers a data sharing agreement as a good

[60] See note [15] at page 19.
[61] This may also interfere with the DMA's policy objectives to promote competition, where potential competitors' data uses may be made dependent on gatekeepers' permission.
[62] Information Commissioner's Office, Data Sharing: A Code of Practice – Security.

practice, even if not strictly mandatory.[63] This agreement must include oversight and review mechanisms to escalate any issues and ensure that the parties act in accordance with the agreement. In case anonymised data is shared, such an agreement can prohibit the recipients of data from re-identifying any individual to whom the data relates and also contain the obligation for the recipients to assess the risks of re-identification on an on-going basis. The UK ICO sees the data sharing agreement as an important accountability instrument - to demonstrate compliance with the GDPR, to set the applicable standards, to include data specification that may include permissions to certain data items, to define the relevant procedures for compliance with individual rights and more generally to allocate responsibilities between the parties. It is unclear whether such an agreement would be recommended as well in the context of the DMA, although it is likely to be used in by the parties in any case and considered a good practice. Finally, the consequences of a situation where the parties would be unable to agree on the terms of the data sharing agreement would also need to be better understood.

2.9 Data subject rights

Individuals have the right to certain information, the right to request access to, rectify or update their data, the right to restrict the processing and the right to ask for deletion or object to the processing. They also have the right to report their data as well as the right not to be subject to a decision based solely on automated processing. The way to exercise these rights has to be made transparent to individuals. These rights have to be ensured throughout the entire data chain, which means they apply to the gatekeepers as well as any other recipient of personal data that acts as a controller of that data (including their processors' obligation to assist). In 2014, the French competition authority (FCA) required GDF Suez (the former French gas supplier monopoly) to disclose part of its consumer database with its competitors. The FCA considered the database and the marketing resources inherited from GDF's former monopoly were necessary for other companies to enter the market and to ensure effective competition. The FCA consulted the French CNIL who concluded that the data to be disclosed to competitors had to be strictly necessary for them to propose their offers to clients. The CNIL also asked the FCA to require GDF to inform its clients before disclosing the data and to propose an opt-out mechanism with clear information to individuals on their right to object within 30 days.[64] Similarly, in August 2015, the UK ICO advised the UK competition authority to invite households who had not switched energy suppliers for three years or more to opt out of having their details shared with rival suppliers.[65] While predating GDPR, these cases remain fully relevant in the context of the DMA and highlight the need for the DMA to include robust regulatory dialogue between the Commission and gatekeepers and potential gatekeepers.

In addition, the GDPR requires the data sharing organisation to inform the recipients of data of any rectification, erasure or restriction of the personal data that has been shared, unless this proves impossible or involves disproportionate effort.[66] The extent to which gatekeepers would have to comply with these obligations and how they should comply remains to be defined. Gatekeepers will also have to be ready to address individuals' queries or complaints about the sharing of their personal data, in case they disagree with it or consider it is affecting them negatively. This may require substantive resources

[63] Information Commissioner's Office, Data Sharing: A Code of Practice – Data Sharing Agreements.
[64] Autorité de la Concurrence, 9 September 2014, Gas Market.
[65] See Information Commissioner's Office, Competition and Market Authority – Energy Market Investigation: Notice of Possible Remedies, 4 August 2015.
[66] Article 19 of the GDPR.

especially if the gatekeeper has shared data on a large scale as per the DMA or the data covered contains sensitive data.

Finally, the GDPR allows certain restrictions to data subject rights. Most notably, Article 23 of the GDPR enables Union or Member State law to restrict the scope of the rights of data subjects in limited circumstances and under stringent conditions. In particular, such law must contain specific provisions to define the processing at stake, the scope of the restrictions, and the safeguards put in place. No restrictions seem to be applicable to GDPR rights, as the DMA does not make any reference to Article 23 of the GDPR. In addition, it is not clear whether the DMA can be considered as Union law constituting a necessary and proportionate measure in a democratic society to safeguard any of the objectives referred to in Article 23(1) of the GDPR. As a result, organisations would have to share and receive data in full compliance with data subject rights, when acting under the DMA.

2.10 Responsibility and liability

In its EU data strategy,[67] the EU Commission highlights various obstacles that have prevented business-to- business data sharing taking off at scale. These mainly stem from the lack of trust between companies, fears about the handling of the data once it has been transferred to another entity, and possible legal and adverse reputational consequences that may result from data sharing. As data mobility increases, organisations must benefit from clear rules on their responsibilities and not be liable for the breach of privacy or security related to data they have shared in accordance with the DMA's provisions. This clarification is all the more important given the increased representative actions in Europe, including opportunistic and ideologically led class actions. Organisations must have legal certainty regarding any exemptions from liability in case of non-compliance with the GDPR, and any other laws to which the gatekeepers, in particular, may be subject to, such as export control laws that may prohibit any sharing of data with organisations fully or partially owned by a foreign government.

Under the GDPR, the relationship between the gatekeeper and the recipients would most likely qualify as a controller-to-controller data sharing. The responsibilities and liabilities attached to this relationship have not yet been clearly defined by the DPA and the EDPB. The point when the responsibility of the sharing entity stops and the responsibility of the recipient entity starts remains undefined and may also be subject to commercial negotiations. It would be also necessary to further clarify the interpretation of GDPR Article 82(4), which enables the data subject to seek compensation from any controller or processor involved in the same processing. This joint and several liability may need to be adapted to the specific context of mandatory controller-to-controller relationship as created by the DMA. In addition, the EDPB could consider how the concept of "same processing" should be understood in the context of data sharing.

With respect to the GDPR's right to portability, the Article 29 Working Party considers that responsibility and liability generally follow user data to its new destination and that "the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient."[68] The same thinking could apply in the context of the DMA, as the gatekeeper (the sending controller) does not choose the recipient of data either. Once the data has been securely transmitted to the correct recipient, the responsibility of the gatekeeper

[67] EU Commission, Communication: A European Strategy for Data, 19 February 2020.
[68] See Note [15] at page 6.

should end. Hence, after the transfer, the gatekeeper should not be responsible for any misuse of personal data by the recipient, nor liable for any data breach by the recipient. At that stage, responsibility would shift to the recipient, who must process the received data in compliance with the GDPR and bear all the attached liabilities.

3. Possible solutions going forward

As demonstrated above, the data sharing provisions of the DMA raise many issues, considerations and uncertainties about implementation and compliance with the GDPR. Some of these require a broader policy consideration, given the important policy goals of both the DMA and the GDPR. Some require a novel interpretation of the GDPR requirements. In any case, any solutions need to be built through multi-stakeholder engagement with the affected businesses and experts in both areas of regulation and with the help of co-regulatory tools, all with the objective of bringing more legal certainty to all actors in the data chain.

3.1 On-going regulatory dialogue and engagement

CIPL highlights the importance of regulatory dialogue to implement the DMA data-sharing objectives properly and in a way that also achieves the full implementation of GDPR's objectives and spirit. This dialogue would enable better informed exchanges of experiences and views and would help regulators better understand market dynamics, technical implications, interests of gatekeepers, data recipients and data subjects, leading to more proportionate and effective outcomes. Although the proposed DMA Recitals prescribe regulatory dialogue,[69] it is important to ensure that such a mechanism is formally developed and implemented, on an ongoing basis and that it is not limited to the context of enforcement. It must include a broader reciprocal, constructive dialogue that results in a complete and robust understanding of digital markets. In that spirit, CIPL supports a duty undertaken by the EU Commission to provide guidelines on the DMA's prohibitions and obligations.[70] Nevertheless, CIPL believes that the Commission can achieve effective outcomes only if the relevant stakeholders also have the chance to provide their expertise and ideas in the process of creating such guidance.

CIPL also stresses the importance of the need for regulatory dialogue with the relevant regulators, in this case, competition and data protection authorities.

Finally, it is essential that any regulatory dialogue includes cross-discipline stakeholders and experts, including technologists, to ensure a plurality of views and break down the regulatory silos.

3.2 Bridging the DMA and the GDPR

Co-regulatory tools and data sharing frameworks - Codes of conduct or data sharing frameworks could specify the rules applicable to data sharing and codify the privacy and security obligations of gatekeepers and recipient organisations in accordance with the applicable laws. The principles and rules of the codes or frameworks should be drafted with the participation of the industry and regulators and in close

[69] The original DMA does not offer any obligation for the EU Commission to engage in a regulatory dialogue. Please see Recitals 33, 58 and 60 Digital Markets Act.
[70] Please note that the European Parliament's adopted DMA prescribes an optional duty to the EU Commission to provide guidelines on the DMA prohibitions and obligations. See, Annex I: European Parliament – Adopted DMA.

consultation with participants in digital markets. They would require entities to implement minimum privacy and security safeguards before sharing and receiving data. Alternatively, the organisations could demonstrate that they already comply with certain market security and privacy standards, such as the ISO ones. The codes would also define the consequences for the relevant organisations for failing to comply with the codes. The codes or frameworks could also contain data-sharing tools, such as data-sharing contract terms templates and examples of organisational measures, frameworks, and technical tools. This would minimise uncertainties and help standardise the sharing of data. The monitoring and enforcement of the codes would be subject to the oversight of a monitoring body[71] working in cooperation with the data protection and competition authorities.

Promoting industry led data mobility projects – Organisations should be encouraged to invest in technical infrastructure and to collaborate to develop open and interoperable standard formats.[72] In its opinions on the DMA and the DGA, the EDPS suggests that the European standardisation organisations should draw up standards on interoperability that should be supported by gatekeepers and supervised by regulators. These standards could include conditions for interoperability, for ensuring the lawfulness of the processing and for facilitating the exercise of individuals' rights.[73] However, CIPL cautions that the digital infrastructure required to support import and export functionalities is technically complex and costly. This technical work could be facilitated by using existing standards rather than creating new ones. For example, the data transfer project for data portability could serve as a model to expand into a broader pro-competitive data mobility standard that is interoperable with standard industry formats, flexible, collaborative and well equipped to deal with future market developments and changes in technology.[74] Such a mobility standard would include established practices in securing access, authorisation and authentication to public APIs as well as encryption in transit. Specific terms would govern the conditions of transferring data into or out of each provider.[75] Such an industry-led standard-setting programme could be set up with the support of and collaboration with regulators. Regulators could also foster similar data-mobility initiatives by mediating discussions about the type of data in the scope of the project, establishing rules on reciprocity and working with industry to investigate the possibility of continuous data transfer.

Regulatory cooperation – To achieve well-functioning digital markets, it is critical to bring different policy and regulatory perspectives together and break the digital silos. Competition law has to take into account its impact on effective data protection. The interpretation and implementation of data protection law

[71] See Article 41 of the GDPR.
[72] See Note [23] pages 83-85. The report calls for further interoperability, including (i) protocol interoperability that ensures that two systems can fully work together and that complementary services can be provided; (ii) data interoperability that enables real-time access for both the data subject and entities acting on his or her behalf; and (iii) full protocol interoperability that ensures that two or more substitute services interoperate.
[73] See Note [10] para 143. Also see Note [28], paras 37-38.
[74] See Note [58].
[75] The following features should be reflected into a future proof data mobility system: (a) Reciprocity: companies wishing to benefit from data mobility schemes should build both import and export functionalities; (b) Privacy and security: the more users' multihome, the greater the possibility of a data breach. Companies should put in place appropriate technical measures to protect the users' data, including during transmission, and to avoid unauthorised access; (c) Ecosystem architecture: The complex technical work required for a data mobility mechanism can be facilitated by finding solutions that enable companies to implement data import and export functionality without changing their core infrastructure; and supporting infrastructure that is flexible enough to be hosted by any service. See Note [58].

should take into account its effects on competition. These debates should not take place in isolation.[76] Formalised cooperation between DPAs and competition authorities is critical to build solutions that enable both a well-functioning competitive market and effective data protection. When both objectives cannot be fully achieved, regulators have to work together to understand and agree on the trade-offs to be made. In the context of the DMA, they could also work together and with industry to produce a toolkit and data sharing framework to enable effective GDPR compliance. The EDPS has launched a digital clearinghouse to facilitate dialogue and cooperation between regulatory authorities and policy makers in order to achieve more coherent protection of individuals in the digital economy across different legal regimes.[77] CIPL supports this initiative and suggests it be developed and deployed in a more systematic manner with a specific focus on the interplay between competition law and the GDPR. The recently established UK Digital Regulation Cooperation Forum (DRCF) could also serve as an example of effective and action-driven regulatory cooperation to address challenges specific to digital and online services.[78] For example, the DRCF work plan for 2021/2022 involves pooling of expertise and resources, working jointly on online regulatory matters and reporting results annually.[79] Finally, some EU Member States, such as Netherlands, are replicating the UK experience and setting up a similar regulatory cooperation forum.[80]

Regulatory sandbox – CIPL has been supporting and encouraging the development of innovative regulatory tools, such as a regulatory sandbox and policy prototyping in the context of both GDPR / data protection and EU AI Act / AI technologies. [81] The interplay between data sharing provisions of DMA and GDPR and the creation of a data sharing framework would be a perfect candidate for a regulatory sandbox or policy prototyping with the relevant regulators. This should be specifically encouraged and envisaged in the DMA and constructed to work across the competition and data protection regulators, too.

Resolving key GDPR issues – Some GDPR provisions and the lack of harmonisation in their interpretation create legal uncertainty for organisations that may generate reticence to engage in data sharing. To address this, EU DPAs – acting via the EDPB - should consult with wider stakeholders to provide a consistent and pan-EU definition and interpretation of anonymous data, which can be implemented in practice, giving confidence to organisations that they can share and receive anonymous data, including in the context of the DMA. The legal regime applicable to pseudonymous data should also be clarified to enable further data mobility. DPAs should also have a more progressive interpretation of the GDPR in general – one that seeks to protect personal data while promoting data mobility, responsible data sharing and the enablement of the EU data economy. For instance, the interpretations of using data for "not incompatible" purposes should be relaxed. Risk assessments and DPIAs should also include the benefits of processing and reticence risk to counterbalance the sole focus on the risks to individuals in DPIAs. There should be a wider debate to explore a constructive way forward to resolving tensions created between

[76] See Note [23], page 76.
[77] Digital Clearinghouse Project.
[78] The Digital Regulation Cooperation Forum (DRCF).
[79] United Kingdom Policy Paper, Digital Regulation Cooperation Forum Work Plan 2021/22.
[80] Autoriteit Persoonsgegevens, Dutch Regulators Strenghten Oversight of Digital Activities by Intensifying Cooperation, 13 October 2021, available at and https://www.acm.nl/en/publications/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation (for Authority for Consumers & Markets Official Statement).
[81] CIPL Regulatory Sandbox White Paper - Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice; CIPL Recommendations on Adopting a Risk-Based Approach to Regulating AI in the EU, and CIPL Response to the EU Commission's Consultation on the Draft AI Act

the GDPR and several other digital initiatives, such as the e-Privacy Regulation, the Artificial Intelligence Act, the DGA, the DMA and sectoral initiatives such as PSD2.[82] This is much needed and would be welcomed by many businesses in the EU, including the SMEs and start-ups.

3.3 Further promoting voluntary data sharing

CIPL welcomes the current EU initiatives to set up the legal framework to promote data sharing in government-to-business, business-to-government and business-to-business contexts.[83] While organisations generally support data mobility,[84] CIPL suggest the additional initiatives below could further encourage the voluntary release of useful, anonymised datasets and overall data mobility within the EU.

Public accreditations for data openness – Regulators (or other relevant public bodies) could offer rewards or endorsements to companies that practice data openness and responsible data sharing.[85] Accreditations of "good actors" could be applied in the area of data openness where potential recipients of user data could demonstrate, through certification to an independent body, that they meet the data protection and processing standards required by the GDPR.[86] Accredited entities could then be identified with a seal and would be eligible to receive data from transferring service providers. Companies would value official endorsements, given the importance of consumer trust in this sector and the reputational benefits that such endorsements would carry. The independent body (potentially in consultation with relevant regulators) could work to assess compliance of certifying entities, revoking certification where appropriate.

---

[82] See Note [35] pages 6-7.

[83] See Note [17] and Data Act and amended rules on the legal protection of databases.

[84] For instance, Google has made datasets publicly available on a large scale over the past decade. For example, Google Trends and Google Correlate both launched in 2011. Google Trends provides data and statistics on the popularity of top search queries in Google Search across various regions and languages (see https://trends.google.com/trends/). Google Correlate complements Google Trends by providing data on how strongly the frequency of multiple search terms correlates with each other over a specified time interval (see https://www.google.com/trends/correlate/). In 2015, Google released Tensor Flow – a popular machine learning software that has been downloaded more than 30 million times and attracted over 17,000 contributors. In 2016, Google released the Open Images dataset, comprising 9 million URLs to images that have been annotated with labels spanning over 6,000 categories, with a view to facilitating machine learning. Google has produced the Google Earth Engine, which enables scientific analysis and visualisation of geospatial datasets, for uses including detecting changes, mapping trends, and quantifying differences on the Earth's surface. There are many other projects too (Google donated N-grams, ImageNet, and YouTube-8M, and frequently collaborates with central banks to provide economically relevant search data using Google Trends). Google's more than 2,000 open source projects are hosted – freely and readily accessible at https://opensource.google/.Facebook Research also disseminates publicly available datasets and research, e.g., Data for Good: New Tools to Help Health Researchers Track and Combat Covid-19, available at https://about.fb.com/news/2020/04/data-for-good/. IBM also provides access to several datasets, including weather and Covid-19, for enterprise data science, available at https://developer.ibm.com/exchanges/data/. For Amazon AWS public data sets, see https://registry.opendata.aws/. For Microsoft Research Open Data, see https://msropendata.com/.

[85] For example, Ofcom, the UK communications regulator, offers accreditations to price comparison sites that agree to undergo "a rigorous independent audit" that "checks on how the site works and checks whether the information provided to consumers is accessible, accurate, transparent, comprehensive, and up to date."

[86] In that regard, the recently approved EU Cloud Code of Conduct can be a useful exemplary tool that enables cloud-computing services to receive official approval from data protection authorities to ensure and demonstrate GDPR compliance.

Supporting data pooling among organisations – In order to increase data sharing practice, regulators could promote existing collaborative practices and tools, such as Open Data Agreements.[87] Standardised data sharing agreements can facilitate collaborative approaches for sharing data resources and have the potential to reduce transaction costs and licensing uncertainty dramatically. In particular, some agreements implement arrangements to ensure that downstream recipients of data can freely use, modify or analyse data.

Furthermore, regulators (or other relevant public bodies) could facilitate cooperation among smaller or nascent digital players that want to pool their respective datasets and thereby achieve greater scale. To facilitate pro-competitive arrangements that help new entrants build up their datasets and to address concerns about perceived antitrust risks, a new block exemption could be introduced to create a safe harbour for data-pooling arrangements, similar to those that exist for vertical agreements, technology transfers, and insurance of motor vehicles. Competition authorities could also offer 'comfort letters' in respect to cooperation agreements that it believes will enhance smaller players' ability to build up useful datasets. The European Commission Special Advisers' report notes this possibility, stating that "*as experience with the assessment of data sharing and data pooling arrangement grows, the Commission may need to contemplate adoption of a block exemption Regulation.*"[88] A useful example and analogy can be found in the European Commission providing informal 'comfort' with respect to a network sharing arrangement concerning the rollout of 5G in Italy, in March 2020.[89]

[87] For instance, the Community Data License Agreements provides a cross-sectoral data license agreement available for widespread use.
[88] See Note [23], Competition Policy for the Digital Era, page 98.
[89] European Commission, Mergers: Commission Clears Acquisition of Joint Control Over INWIT by Telecom Italia and Vodafone, Subject to Conditions. 6 March 2020.

Appendix 1 – Relevant Draft Provisions by the EU Commission and Adopted Amendments by the European Parliament of the DMA with Data Privacy Impact

TOPIC	DMA EC PROPOSAL
Definitions of data and personal data	**Article 2** (19) 'Data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording; (20) 'Personal data' means any information as defined in point 1 of Article 4 of Regulation (EU) 2016/679; (21) 'Non-personal data' means data other than personal data as defined in point 1 of Article 4 of Regulation (EU) 2016/679.
Gatekeepers are required to refrain from combining data unless the end-user has consented	Article 5(a) Obligations for gatekeepers … a gatekeeper shall: refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679. **Recital (36)** The conduct of combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry. To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised alternative. The possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third party websites, and should be proactively presented to the end user in an explicit, clear and straightforward manner.
Gatekeepers are required to provide tools to end-users to facilitate exercise of the data portability rights, including by the provision of continuous and real-time access.	**Article 6(1)(h)** … a gatekeeper shall … provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access. **Recital (54)** Gatekeepers benefit from access to vast amounts of data that they collect while providing the core platform services as well as other digital services. To ensure that gatekeepers do not undermine the contestability of core platform services as well as the innovation potential of the dynamic digital sector by restricting the ability of business users to effectively port their data, business users and end users should be granted effective and immediate access to the data they provided or generated in the context of their use of the relevant

	core platform services of the gatekeeper, in a structured, commonly used and machine-readable format. This should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that business users and end users can port that data in real time effectively, such as for example through high quality application programming interfaces. Facilitating switching or multi-homing should lead, in turn, to an increased choice for business users and end users and an incentive for gatekeepers and business users to innovate.
Gatekeepers are required to provide business users with effective, high quality, continuous and real-time access and use of aggregated and non-aggregated data that is provided for or generated in the context of the use of core platform services. For personal data, gatekeepers are required to provide such access and use where directly connected with the use by the end user in respect of the products or services offered by the business user through the core platform services, and when the user gives GDPR consent.	**Article 6(1)(i)** … a gatekeeper shall … provide business users, or third parties authorised by a business user, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data, that is provided for or generated in the context of the use 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; for personal data, provide access and use only where directly connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end user opts in to such sharing with a consent in the sense of the Regulation (EU) 2016/679; **Recital (55)** Business users that use large core platform services provided by gatekeepers and end users of such business users provide and generate a vast amount of data, including data inferred from such use. In order to ensure that business users have access to the relevant data thus generated, the gatekeeper should, upon their request, allow unhindered access, free of charge, to such data. Such access should also be given to third parties contracted by the business user, who are acting as processors of this data for the business user. Data provided or generated by the same business users and the same end users of these business users in the context of other services provided by the same gatekeeper may be concerned where this is inextricably linked to the relevant request. To this end, a gatekeeper should not use any contractual or other restrictions to prevent business users from accessing relevant data and should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required under Regulation (EU) 2016/679 and Directive 2002/58/EC. Gatekeepers should also facilitate access to these data in real time by means of appropriate technical measures, such as for example putting in place high quality application programming interfaces.
Gatekeepers are required to provide third-party search engines fair, reasonable and non-discriminatory access to ranking, query, click and view data in relation to free and paid searches by end users on search engines of the gatekeeper,	**Article 6(1)(j)** … a gatekeeper shall … provide to any third party providers of online search engines, upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online

subject to anonymisation where the data constitutes personal data.	search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data; **Recital (56)** The value of online search engines to their respective business users and end users increases as the total number of such users increases. Providers of online search engines collect and store aggregated datasets containing information about what users searched for, and how they interacted with, the results that they were served. Providers of online search engine services collect these data from searches undertaken on their own online search engine service and, where applicable, searches undertaken on the platforms of their downstream commercial partners. Access by gatekeepers to such ranking, query, click and view data constitutes an important barrier to entry and expansion, which undermines the contestability of online search engine services. Gatekeepers should therefore be obliged to provide access, on fair, reasonable and non-discriminatory terms, to these ranking, query, click and view data in relation to free and paid search generated by consumers on online search engine services to other providers of such services, so that these third-party providers can optimise their services and contest the relevant core platform services. Such access should also be given to third parties contracted by a search engine provider, who are acting as processors of this data for that search engine. When providing access to its search data, a gatekeeper should ensure the protection of the personal data of end users by appropriate means, without substantially degrading the quality or usefulness of the data.
Any measures implemented to comply with Articles 5 and 6 must comply with the GDPR and ePrivacy Directive.	**Article 7(1)** The measures implemented by the gatekeeper to ensure compliance with the obligations laid down in Articles 5 and 6 shall be effective in achieving the objective of the relevant obligation. The gatekeeper shall ensure that these measures are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety. **Recital (58)** To ensure the effectiveness of the obligations laid down by this Regulation, while also making certain that these obligations are limited to what is necessary to ensure contestability and tackling the harmful effects of the unfair behaviour by gatekeepers, it is important to clearly define and circumscribe them so as to allow the gatekeeper to immediately comply with them, in full respect of Regulation (EU) 2016/679 and Directive 2002/58/EC, consumer protection, cyber security and product safety. The gatekeepers should ensure the compliance with this Regulation by design. The necessary measures should therefore be as much as possible and where relevant integrated into the technological design used by the gatekeepers. However, it may in certain cases be appropriate for the Commission, following a dialogue with the gatekeeper concerned, to further specify some of the measures that the gatekeeper concerned should adopt in order to effectively comply with those obligations that are susceptible of being

	further specified. This possibility of a regulatory dialogue should facilitate compliance by gatekeepers and expedite the correct implementation of the Regulation.
The Commission may require a gatekeeper to implement specific measures under Article 7(1).	**Article 7(2)** Where the Commission finds that the measures that the gatekeeper intends to implement pursuant to paragraph 1, or has implemented, do not ensure effective compliance with the relevant obligations laid down in Article 6, it may by decision specify the measures that the gatekeeper concerned shall implement. The Commission shall adopt such a decision within six months from the opening of proceedings pursuant to Article 18. **Recital (58)** To ensure the effectiveness of the obligations laid down by this Regulation, while also making certain that these obligations are limited to what is necessary to ensure contestability and tackling the harmful effects of the unfair behaviour by gatekeepers, it is important to clearly define and circumscribe them so as to allow the gatekeeper to immediately comply with them, in full respect of Regulation (EU) 2016/679 and Directive 2002/58/EC, consumer protection, cyber security and product safety. The gatekeepers should ensure the compliance with this Regulation by design. The necessary measures should therefore be as much as possible and where relevant integrated into the technological design used by the gatekeepers. However, it may in certain cases be appropriate for the Commission, following a dialogue with the gatekeeper concerned, to further specify some of the measures that the gatekeeper concerned should adopt in order to effectively comply with those obligations that are susceptible of being further specified. This possibility of a regulatory dialogue should facilitate compliance by gatekeepers and expedite the correct implementation of the Regulation.
Where data subject consent is required to ensure compliance with the DMA, a gatekeeper must enable business users to directly obtain the consent required for their processing, or to comply with data protection law in other ways, such as by providing anonymous data where appropriate. Gatekeepers must not make it more difficult for business users to obtain consent than it is for the gatekeeper.	**Article 11(2)** Where consent for collecting and processing of personal data is required to ensure compliance with this Regulation, a gatekeeper shall take the necessary steps to either enable business users to directly obtain the required consent to their processing, where required under Regulation (EU) 2016/679 and Directive 2002/58/EC, or to comply with Union data protection and privacy rules and principles in other ways including by providing business users with duly anonymised data where appropriate. The gatekeeper shall not make the obtaining of this consent by the business user more burdensome than for its own services.
The Commission may involve gatekeepers in a regulatory dialogue in the context of enforcement framework.	**Recital (33)** The obligations laid down in this Regulation are limited to what is necessary and justified to address the unfairness of the identified practices by gatekeepers and to ensure contestability in relation to core platform services provided by gatekeepers. Therefore, the obligations should correspond to those practices that are considered unfair by taking into account the features of the digital sector and where experience gained, for example in the enforcement of the EU competition rules, shows that they have a particularly negative direct

	impact on the business users and end users. In addition, it is necessary to provide for the possibility of a regulatory dialogue with gatekeepers to tailor those obligations that are likely to require specific implementing measures in order to ensure their proportionality and effectiveness. **Recital (58)** To ensure the effectiveness of the obligations laid down by this Regulation, while also making certain that these obligations are limited to what is necessary to ensure contestability and tackling the harmful effects of the unfair behaviour by gatekeepers, it is important to clearly define and circumscribe them so as to allow the gatekeeper to immediately comply with them, in full respect of Regulation (EU) 2016/679 and Directive 2002/58/EC, consumer protection, cyber security and product safety. The gatekeepers should ensure the compliance with this Regulation by design. The necessary measures should therefore be as much as possible and where relevant integrated into the technological design used by the gatekeepers. However, it may in certain cases be appropriate for the Commission, following a dialogue with the gatekeeper concerned, to further specify some of the measures that the gatekeeper concerned should adopt in order to effectively comply with those obligations that are susceptible of being further specified. This possibility of a regulatory dialogue should facilitate compliance by gatekeepers and expedite the correct implementation of the Regulation. **Recital (60)** In exceptional circumstances justified on the limited grounds of public morality, public health, or public security, the Commission should be able to decide that the obligation concerned does not apply to a specific core platform service. Affecting these public interests can indicate that the cost to society as a whole of enforcing a certain obligation would in a certain exceptional case be too high and thus disproportionate. The regulatory dialogue to facilitate compliance with limited suspension and exemption possibilities should ensure the proportionality of the obligations in this Regulation without undermining the intended ex ante effects on fairness and contestability.

TOPIC	
EUROPEAN PARLIAMENT TEXT OF Art 36(a) [*new*] as voted on 23.11.2021	***Article 36(a) - Guidelines*** *To facilitate the compliance of gatekeepers with and the enforcement of the obligations in Articles 5,6, 12 and 13, the Commission ~~shall~~ may accompany the obligations set out in those Articles with guidelines, where the Commission deems that this is appropriate. Where appropriate and necessary, the Commission may mandate the standardisation bodies to facilitate the implementation of the obligations by developing appropriate standards.*

Appendix 2 - Data Transfer Project Overview and Fundamentals - July 20, 2018[90]

Shared Responsibilities Table: Security and Privacy

Task	User	Provider-exporter	Provider-Importer	Hosting Entity	DTP System
Data Minimization	Selects data to transfer	Provides granular controls of what data to export	Discards any data not needed for their service	Configure only appropriate transfer partners	N/A
Rate Limiting	N/A	Implements	N/A	Sets reasonable limits to prevent abuse	Supports provider-specific rate limiting
User Notification	Receives and reviews notification of transfer	N/A	N/A	Configure mail sender and delay policy	Send notification, optionally with delay to allow for cancellation
Token Revocation	May need to manually revoke tokens if provider doesn't support automated revocation	Support Token Revocation	Support Token Revocation	N/A	Revoke Auth tokens after use (if supported by providers)
Minimal Scopes for Auth Tokens	Verify Appropriate Scopes requested	Implements granular scopes	Implements granular scopes	N/A	Requests minimal scopes for each transfer
Data Retention	Transfer of data is not deletion, user should delete source data if desired	Store only data needed to prevent fraud and abuse	Only retain imported data in compliance with privacy policies; Store metadata needed to prevent fraud and abuse	Configures system to not retain any identifiable information	Retains no data after transfer completed
Abuse	Protect account credentials (strong passwords, two-factor authentication, etc.)	Implement appropriate fraud and abuse protections on APIs	Implement appropriate fraud and abuse protections on APIs	Implement appropriate fraud and abuse protections on UI	Encrypts data in transit and at rest using ephemeral key; Uses isolated/dedicated VMs per transfer

[90] See Note [58], Data Transfer Project Website White Paper.