Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences

Discussion Paper | May 2023

Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences

Contents

Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences

The Centre for Information Policy Leadership ("CIPL")[1] has been a leader in promoting the responsible use of data for more than 20 years. CIPL supports the goals of the European Union's ("EU") Digital Strategy fostering innovation, growth and competitiveness in the EU while establishing safe and trusted digital spaces for individuals. As part of CIPL's ongoing project examining the Digital Markets Act ("DMA"),[2] CIPL is publishing a series of papers taking a closer look at potential implementation challenges and remaining legal uncertainties across the complete EU digital legislation package. In the first paper, CIPL provided an overview of the data protection implications of the DMA.[3] This second paper will take an in-depth look at open questions regarding the seeming limitation by the DMA of legal bases available for certain processing of personal data and whether the DMA should consequently be considered as a *lex specialis* to the GDPR. Additionally, the paper examines ambiguities related to the scope of DMA in terms of personal data processing and lack of definitions of 'data combination' and 'cross-use.'

Finally, this paper provides a set of recommendations and a suggested way forward to interpret the DMA provisions as they relate to the GDPR legal basis provisions in a way that doesn't contradict nor erode the spirit and the intent of both laws.

CIPL conclusions and recommendations

- Explicitly note that the DMA is not *lex specialis* to the GDPR
- Provide a clear affirmation that the scope of the DMA is limited to "removing obstacles from the internal market" and does not limit the applicability of the GDPR, including to the processing of personal data otherwise in the scope of the DMA
- Provide clear guidance as to whether DMA consent is equivalent or concurrent to GDPR consent as a legal basis for personal data processing

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

[2] CIPL has previously published a White Paper on "*Bridging the DMA and the GDPR—Comments by the CIPL on the Data Protection Implications of the Draft DMA,*" analysing the relationship between the Digital Markets Act's data sharing obligations and the GDPR's data protection requirements.

[3] CIPL has previously published a White Paper on "Bridging the DMA and the GDPR—Comments by the CIPL on the Data Protection Implications of the Draft DMA," analysing the relationship between the DMA's data sharing obligations and the GDPR's data protection requirements.

- Further define what constitutes data combination and cross-use of personal data in the context of DMA
- Provide use cases for the application of Art. 6(1), points (c), (d) or (e) GDPR legal basis in the context of DMA data combination and cross-use of personal data
- Ensure that the DMA fulfils its promise of reducing fragmentation across Member States' approaches to competition law enforcement in digital markets and bolster cooperation between competition and data protection authorities

1 INTRODUCTION

The limitations of legal bases otherwise available under the GDPR for specific processing of personal data by the DMA raises the question of the general relationship between the DMA and GDPR, specifically, whether the DMA should be considered as *lex specialis* to the GDPR in certain cases.

The European Union is subject to detailed, complex and strict rules and limitations on its law-making activities. In particular, the EU can act only within the scope of competences that the Member States have conferred upon it in the treaties to attain the objectives set out therein.[4] Accordingly, the EU has three forms of competence: exclusive, shared and supplementary, set out in Articles 3, 4 and 6 of the Treaty on the Functioning of the European Union ("TFEU").[5] Any competence not conferred upon the EU in the Treaties remains with individual member states. In addition, Article 5 of the Treaty on European Union ("TEU") clarifies that any EU competence is governed and limited by the fundamental principles of proportionality and, for non-exclusive competencies, subsidiarity.[6]

To determine the relationship between the DMA and GDPR, CIPL looked at the legal basis on which the co-legislator relied for the DMA, i.e., Article 114 of the TFEU. Article 114 TFEU empowers legislators to adopt measures that are designed to approximate national rules and prevent regulatory fragmentation in the internal market, also known as the harmonisation clause.[7]

[4] Article 5(2) of the Treaty on European Union (TEU).
[5] Treaty on the Functioning of the European Union, 2012/C 326/01.
[6] Article 5 of the Treaty on European Union, C326/13. *"(3) Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at the regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. (4) Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties."*
[7] Article 114 of the TFEU and the Preamble of the Regulation 2022/1925 on contestable and fair markets in the digital sector ("Digital Markets Act").

2 THE DMA IS NOT *LEX SPECIALIS* TO THE GDPR

Under Article 3(1)(b) of the TFEU, the EU has the exclusive competence to establish competition rules necessary for the functioning of the internal market. The internal market is a cornerstone of the overall functioning of the EU, encompassing four freedoms, i.e., free movement of goods, free movement of capital, freedom to establish and provide services and free movement of people. Generally, it is therefore not uncommon for legislative initiatives to be based on Article 114 (1) TFEU alone, where a measure does not fit into more specific treaty provisions.[8]

Article 114(1) TFEU

"(. . .) [t]he European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."

The Court of Justice of the European Union ("CJEU") jurisprudence places a clear boundary around Article 114 TFEU as a legal basis though requiring a link between the measure adopted and the elimination of an identified obstacle to the internal market.[9] Specifically, reliance on Article 114 TFEU as a legal basis can be justified where the measure at issue (i) genuinely improves the conditions for the establishment and functioning of the internal market and (ii) there are differences between national rules obstructing fundamental freedoms that have a direct effect on the functioning of the internal market or cause significant distortions of competition.

According to the DMA Impact Assessment Report[10] and its Explanatory Memorandum,[11] Article 114 TFEU is considered the relevant legal basis due to (i) the intrinsic cross-border nature of the services provided by gatekeepers and (ii) the risk of further fragmentation regarding the functioning of the

[8] Alina Kaczorowska-Ireland clarifies that Article 114 is not a catch-all provision, and specific requirements can be derived from CJEU's case-law on its use. See, Alina Kaczorowska-Ireland *European Union Law* (4th Ed., Routledge:2016): 186-188. Also, Paul Craig and Gráinne de Búrca share their concerns about the misuse of article 114 *in EU Law: Text, Cases and Materials* (7th Ed., Oxford University Press: 2020): 123 and 124.

[9] See Case C-58/08 *Vodafone, O2 et al v Secretary of State*, EU:C:2010:321, paras 32. Also, Case C-491/01 *British American Tobacco (Investments) and Imperial Tobacco* [2002] ECR I-11453, para 60.

[10] European Commission, Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363 final, part 1/2.

[11] Proposal for a Regulation of the European Parliament and Of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act).

Single Market for digital services. The Impact Assessment Report further includes a more detailed chapter which examines rules with the potential to affect the functioning of digital platforms. The provided analysis identifies solely competition law-related instruments at the Member States' national level and concludes that: "the current rules in place already create a certain degree of distortion of competition between the Member States insofar as the rules on tackling unfairness in dependency relationships diverge as to the preconditions to intervene and as to the depth of intervention."[12]

2.1 Data Protection Provisions Throughout the DMA

The DMA contains numerous provisions which directly reference the application of data protection law.[13] For instance, it explicitly excludes Article 6 (1) GDPR points *(b) necessary for the performance of a contract* as well as *(f) necessary for the purpose of the legitimate interest pursued by the controller or a third party* from the selection of possible legal basis for data combination and cross-use. Considering that the DMA is to apply *without prejudice* to the GDPR, this raises the question of whether the DMA has primacy over the GDPR where the processing of personal data for any data combination or cross-use of data is concerned and whether this would mean that the DMA is to be considered *lex specialis* to the GDPR. Several considerations speak against this interpretation, however.

2.1.1 Article 114 TFEU as the Single Legal Basis

In other legal instruments, such as the proposals for the AI Regulation and the e-Privacy Regulation, the European legislator appears to have considered this issue carefully.[14]

- While the e-Privacy Directive, which was adopted before the Treaty of Lisbon, is based on Article 95 of the Treaty establishing the European Community (the equivalent to current Article 114 TFEU), the post-Treaty of Lisbon proposal for an e-Privacy Regulation uses a double legal basis of Article 16 TFEU (protection of individuals regarding the processing of personal

[12] European Commission, Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363 final, part 2/2, chapter *Existing Fragmentation Resulting from Divergencies in the Laws of MS Addressing Economic Power of Digital Platforms* p. 111.

[13] See CIPL Paper on *"Bridging the DMA and the GDPR—CIPL Comments on the Data Protection Implications of the Draft Digital Markets Act,"* December 6, 2021, available here.

[14] Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. Also, the Proposal for a Regulation concerning respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

data) and Article 114 TFEU.[15] From the Commission's Explanatory Memorandum, it is clear that the proposal for an e-Privacy Regulation pursues a twofold objective: ensuring personal data protection and developing a single market.[16] These choices are not incidental since a double legal basis is required to fulfil the twofold objectives of the Regulation.

- The proposal for the Artificial Intelligence Act is based on Articles 114 and 16 TFEU, and the proposal explicitly notes that it contains specific rules on the protection of individuals regarding the processing of personal data.

The DMA, on the other hand, is not supported by a double legal basis. Relying on Article 16 TFEU,[17] in addition to Article 114 TFEU, might have been an indication that the lawmakers intended to directly regulate the processing of personal data.[18] Article 114 TFEU and the protection of the single market do not establish primacy over Article 16 TFEU. Any other interpretation, in addition to conflicting with the intent expressed in Recital 12 of the DMA, would potentially also conflict with Article 52 of the Charter of Fundamental Rights of the European Union.[19] Instead, the Recital 12 of the DMA simply clarifies that the DMA applies without prejudice to the rules of the General Data Protection Regulation ("GDPR"), without further clarification for organisations ultimately subject to the DMA how to apply both laws in parallel.[20] Additionally, the DMA Impact Assessment

---

[15] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and relating Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), see page 3 (Legal Basis).

[16] Regulation 2017/0003 Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC, Explanatory Memorandum.

[17] Article 16 TFEU states that everyone has the right to the protection of personal data concerning them. The article also prescribes the ordinary legislative procedure as a means to enacting rules relating to the protection of individuals with regard to the processing of personal data.

[18] For instance, the proposed Artificial Intelligence ("AI") Act relies on Articles 16 and 114 TFEU. The AI Act Explanatory Memorandum notes that: "*the legal basis for the proposal is in the first place Article 114 TFEU, which provides for the adoption of measures to ensure the establishment and functioning of the internal market*" and "*in addition, considering that this proposal contains certain specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU.*" See the AI Act Explanatory Memorandum, page 6.

[19] Article 8 of the EU Charter acknowledges that everyone has the right to the protection of personal data concerning him or her. Moreover, Article 52 of the EU Charter regulates the scope and interpretation of the Charter, stating that, (1) *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. (2) Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.*

[20] CIPL Paper on "*the DMA and the GDPR,*" page 3. Please also see Case C-162/97, Nilsson and others, para 54, which states that "*(. . .) the preamble to a Community act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question.*"

contains a review of the various policy options considered in the process of preparing a legislative proposal for DMA. The assessment concerning the coherence of the given policy options, including the option on which the DMA is currently based, with other EU regulatory instruments, notes that: "*All options complement the data protection laws. Transparency obligations on deep consumer profiling will actually help inform GDPR enforcement, whereas mandatory opt-out for data combination across core platform services goes beyond GDPR protections.*"[21]

Finally, Article 114 TFEU as a single legal basis has further limitations, namely:

- the Article's specific aim is to remove obstacles from the internal market and
- a more specific legal basis that can be used for the adoption of the measures should not exist.

In this specific case, a more specific legal basis, i.e., regulating data protection pursuant to Article 16 TFEU, certainly exists. The EU case law dictates that any issues relating to the protection of personal data processing should be resolved on the basis of the relevant provisions governing data protection.[22] Therefore, DMA is not lex specialis to the GDPR but exists in parallel.

2.1.2 Compatibility of DMA and GDPR Consent

It is also unclear, in this context, how consent under the Article 5(2) of the DMA to legitimise certain data processing activities relates to the legal basis for the processing of personal data under Article 6 (1)(a) GDPR - consent. Article 5(2) DMA only states: "Unless the end-user has been presented with the specific choice and has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679." The referenced GDPR articles define, and set conditions for consent, but Article 5 DMA does not, for instance, reference consent under Article 6(1) or 9(1) in the sense of a legal basis. Similarly, Recital 37 DMA makes reference to the way consent has to be provided (by a clear affirmative action) *as defined* under the GDPR but does not directly equate the two.

---

[21] Commission Staff Working Document, Impact Assessment Report: Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), para 363.

[22] 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. All judgments note that personal data are not, as such, a matter for competition law, nor that any privacy-related concerns flowing from the increased concentration of data within the control of one company fall within the scope of EU competition law.

One conclusion to draw from that is consent under the DMA is, in fact, an additional, separate consent from the GDPR consent for data processing. Leaving practical considerations as to how this would be set up in practice aside (i.e., separate consent screens with potentially different choices), one might presume that where consent is required under the DMA, GDPR consent could also be obtained (although that may not, in every case, be the desired legal basis). It is also difficult to see how consent to be obtained under the DMA could be a condition of a contract in accordance with Article 6 (1) point b GDPR for a user to allow data combination and cross-use of data. This consideration would also apply to legitimate interest—it is difficult to see how Articles 6(1)(b) or (f) GDPR could be combined with a separate DMA consent.

However, Article 13(5) DMA makes reference to consent for cross-using (not data combination) to ensure compliance with *this Regulation* (meaning the DMA). It then continues to qualify this with: "where that consent is required under regulation (EU) 2016/679. . .", seemingly linking both consents together after all. The Commission should, therefore, clarify how the DMA consent was intended to relate to consent as a legal basis for the processing of personal data under the GDPR.

3 PROHIBITION OF DATA COMBINATION AND CROSS-USE OF PERSONAL DATA MUST BE TIED TO THE SCOPE OF THE DMA

As a central provision of the DMA, Article 5(2) expressly prohibits *data combination* and *cross-use* of *personal data* unless one of a limited selection of legal basis under the GDPR that the DMA expressly lists are available to undertakings qualified as gatekeepers, with consent being the preferred option. In other words, the DMA seemingly narrows the legal bases that are normally available in accordance with GDPR for the processing of personal data to a select few when it comes to specific processing activities – data combination and cross-use of personal data.

Digital Markets Act
Article 5(2)

"2. The gatekeeper shall not do any of the following:
(a) [. . .];
(b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services;
(c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and

(d) sign 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 has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679.
Where the consent given for the purposes of the first subparagraph has been refused or withdrawn by the end user, the gatekeeper shall not repeat its request for consent for the same purpose more than once within a period of one year.
This paragraph is without prejudice to the possibility for the gatekeeper to rely on Article 6(1), points (c), (d) and (e) of Regulation (EU) 2016/679, where applicable."

The DMA thus appears to establish consent as the primary legal basis, leaving "compliance with a legal obligation,"[23] protection of vital interests of the data subject or another natural person,"[24] and "necessary for the performance of a task in the public interest"[25] as potential "back-up" legal bases for specific processing activities.[26] The DMA explicitly excludes the possibility of *data combination* and *cross-use* of personal data where "necessary for the performance of a contract"[27] or where the processing is "necessary for the purpose of the legitimate interest pursued by the controller," legal basis for the processing of personal data otherwise available under the GDPR.[28] This raises several points that require further clarification by the Commission, namely:

- that the DMA is not *lex specialis* to the GDPR as shown above;
- the scope of the DMA in relation to the processing of personal data is limited to "*removing obstacles from the internal market;*"
- defining *data combination* and *cross-use* of data under the DMA must be lined to its scope.

4 LIMITATIONS IN THE SCOPE OF DMA IN RELATION TO PROCESSING PERSONAL DATA

Since we established that the DMA is not *lex specialis* to GDPR, it is evident DMA can only be applicable as far as its legal basis allows, i.e., to "*remove obstacles from the internal market.*" Therefore, where

[23] Article 6 (1) point c GDPR.
[24] Article 6(1) point d GDPR.
[25] Article. 6 (1) point e GDPR.
[26] "Without prejudice to the possibility of the gatekeeper." Apart from consent exception, gatekeepers can also engage in data use and combination activity if the Commission provides exemption pursuant to Article 10 DMA or, in cases of urgency, interim measures pursuant to Article 24 DMA. Such methods can be useful tools for law enforcement agencies while conducting criminal investigations. However, considering the scale and volume of exemption requests potentially made by law enforcement agencies, in the absence of a systemic exemption, such methods will create an excessive and unreasonable administrative burden resulting in an impractical instrument. Besides, it is questionable whether the Commission has or can have the infrastructure to evaluate such volume of exemption requests for data combination practice.
[27] Article 6(1) point b GDPR.
[28] Article 6(1) point f GDPR.

the processing activity is not part of the DMA's intended scope, it must be left to be regulated by the GDPR. In other words, any processing of personal data that falls outside the scope of the DMA may be legitimised under the GDPR.

The way consent is incorporated in the DMA must be seen in light of the objective of the DMA and Article 5(2). The form of choice is intended to ensure that a gatekeeper's data advantage does not substantially undermine the contestability of the core platform services. This is a thoroughly different objective from the GDPR, which is the protection of natural persons with regard to the processing of personal data. As the DMA is intended to apply without prejudice to the GDPR (in line with the explicit intent in the recitals),[29] the GDPR must remain applicable in cases where both the GDPR and the DMA regulate a specific situation. A conflict arises when the DMA prohibits a certain type of processing that would otherwise be permissible under the GDPR. As mentioned above, such a conflict also arises where national rules prohibit a certain type of processing that would otherwise be permissible under the GDPR. Thus, without regulatory or legislative clarification that the GDPR applies in parallel to the DMA, gatekeepers may find it challenging to deliver compliance with some of the DMA and the GDPR obligations.[30]

Other legislative acts in the EU's Digital Strategy package are more clearly structured. For instance, Article 1(3) of the Data Governance Act clearly states that in cases related to personal data, the relevant Union or national law concerning personal data protection prevails. A similar approach is presented in the Data Act proposal, namely Article 1(3). The proposal for the Regulation on the transparency and targeting of political advertising clearly states that it should be considered as *lex specialis* to the GDPR.

Data Governance Act, Article 1(3)

"[it is] is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competencies of

[29] Recital 12 of the Digital Markets Act states that, "*this Regulation should also apply without prejudice to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation, in particular Regulations (EU) 2016/679(4)and (EU) 2019/1150(5)of the European Parliament and of the Council and a Regulation on a single market for digital services, and Directives 2002/58/EC(6), 2005/29/EC(7), 2010/13/EU(8), (EU) 2015/2366(9), (EU) 2019/790(10)and (EU) 2019/882(11)of the European Parliament and of the Council, and Council Directive 93/13/EEC(12), as well as national rules aimed at enforcing or implementing those Union legal acts.*"

[30] CIPL White Paper on Bridging the DMA and the GDPR, page 7.

supervisory authorities. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data shall prevail."
Proposal for a Data Act, Article 1(3) *"Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities."*
Proposal for a Regulation on the transparency and targeting of political advertising, Article 1(4a) **European Parliament amendments text** *The data protection rules on processing of personal data provided for in this Regulation shall be considered as specific data protection rules to the general rules laid down in the Regulations (EU)2016/679 and (EU)2018/1725. None of the provisions in this Regulation can be applied or interpreted in such way as to diminish or limit level of protection offered by the right to respect for private life and protection of personal data and by the right of freedom of expression as protected in the Charter of Fundamental Rights and in the Union law on data protection and privacy, in particular by Regulations (EU)2016/679 and (EU)2018/1725).*

While the DGA and Data Act proposals specifically acknowledge the limited scope of respective obligations in the context of personal data protection, the DMA does not appear to limit its scope vis-a-vis the GDPR more specifically, even though the preamble refers to the same application "without prejudice" to the GDPR.

In addition to the DMA, individual member states are or have already introduced their own competition rules overlapping with the DMA, including with respect to data processing. These rules create further scope for tensions also with the GDPR. In Germany, for instance, the Bundeskartellamt[31] has recently issued a statement of objections against Google that invokes Section 19a GWB to prohibit cross-service data processing without consent.[32]

[31] Bundeskartellamt is Germany's Federal Cartel Office.
[32] Bundeskartellamt press release—Statement of objections issued against Google's data processing terms, 11 January 2023, available at

5 IMPACT ON DATA COMBINATION AND CROSS-USE OF PERSONAL DATA

5.1 Defining Data Combination and Cross-Use of Personal Data

As indicated above, the DMA prohibits combining personal data between individual core platform services, other gatekeepers or third-party services. In the same manner, the DMA also prohibits the cross-use of personal data among gatekeeper services. However, the DMA does not provide any definitions, technical specifications or qualifications on what constitutes combination and cross-use of personal data in this context.

In the data protection context, the UK's Information Commissioner's Office Guidance on Data Protection Impact Assessments made reference, though not specifically in the context of data combination, to data matching that is to be understood as "combining, comparing or matching personal data obtained from multiple sources," pointing towards the impact this type of processing can have on individuals.[33] The EDPBs predecessor, the Article 29 Working Party, also refers to matching or combining datasets as "originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject."[34] Neither can provide clarity as to the specific definitions for data combination or cross-use of data under the DMA, however. Recital 36 DMA makes mention of data combination and cross-use but offers no more specific definitions.

The legislative aim of the DMA is to prevent "unfair practices for business users, as well as for end users of core platform services" "to the detriment of price, quality, fair competition, choice and innovation in the digital sector."[35] In practice, however, "data combination" as well as "cross-use" of data could refer to a number of data processing activities and processing purposes, and it is not immediately clear which would fall under the scope of the DMA. The lack of a clearer definition creates legal uncertainty for gatekeepers and may hinder the development of new services or technology in

https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html.

[33] Information Commissioner's Office, Guidance on Data Protection Impact Assessments (DPIAs), 2018, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/, p. 43.

[34] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 2017, WP248rev.01, p. 10.

[35] Recital 4 of the Digital Markets Act.

the longer run. Finally, it is not evident how a wholesale prohibition of all forms of data combination or cross-data use involving the processing of personal data would, in fact, serve the purpose of Article 114 TFEU.[36]

5.2 Potential implications of DMA data combination and cross-use limitation

A wholesale restriction of data combination under Article 5(2)[37] of the DMA and the limitation to only a specific legal basis under the GDPR does raise concerns for select use cases of data combination or cross-use of data intended to protect either a company's infrastructure or individuals directly.

Concretely, digital products and services often interact, and such interactions will often involve exchanges of user data. Subjecting all such interactions to prior consent requirements would, in many cases, disrupt the proper functioning of digital services and frustrate users. The European legislator seems to have recognised this risk because it allows the cross-use of personal data without consent where services are provided together or in support of each other (Art. 5(2)(c) and Recital 36)). Whether this exception will help avoid unnecessary disruptions will depend critically on where the boundary between "combining" and "cross-using" of personal data is drawn because the exception applies only for cross-using but not combining data. An overly restrictive interpretation of "cross-using" would impair the interoperability and interaction of different products. As a result, gatekeepers would be prevented from offering users who decline consent for cross-service data processing services that are less personalised but of equivalent quality, as Recital 36 demands.

5.2.1 Data Security and Integrity

All organisations need to protect themselves and their users, employees, customers and business partners from unwanted security intrusions, unauthorised access, fraudulent and other criminal activities and cyberattacks. Article 8 (1) of the DMA specifically requires that all measures taken by the gatekeeper, in compliance with Articles 5, 6 and 7, must also comply with any cybersecurity legislation.

---

[36] As explained by Giacomo Delinavelli, *"the EU may [only] intervene [based on Article 114] to cure diversity between national laws only where that diversity is shown to be harmful to the achievement of the EU's internal market."* See Giacomo Delinavelli *"Cybersecurity for Europe without a legal basis?"*, February 1, 2022, available here.

[37] Article 5 (2) point (a) limits the restrictions to the "purpose of providing online advertising" while no such restrictions to specific purposes exists for the data combination and cross-use prohibitions in Article 5 (2).

Continuous threat level assessment is a central tenet of information security,[38] and it inevitably includes the processing of personal data for monitoring and detection.

Data combination and cross-use of data across platform ecosystems constitute one of the most effective tools for data security measures allowing for the identification, detection and prevention of sophisticated criminal activities.[39]

- The cross-platform analysis is routinely used for information security purposes:[40] usernames, ages, e-mail addresses, phone numbers and log-in credentials are often re-used by individuals on different platforms and online settings.[41] For example, a malicious actor using multiple social media platforms to have private message exchanges regarding fraudulent activity may be captured by combining a single identifier across platforms, e.g., account name or phone number.[42]
- In the financial service industry, the software is usually deployed to detect suspicious transactions. In addition, financial services have started to share data across platforms in an effort to detect patterns that would not be evident otherwise within an individual service, for instance.[43]

[38] See, for instance, Principles 6 and 9 of OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY; Enisa Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, p. 12.
[39] For a detailed overview, see Victoria Baines in "Investigating the case for an EU Chief (Information) Security Officer through a close reading of digital regulation and policy," p. 2.
[40] Victoria Baines, "*Investigating the Case for an EU Chief Information Security Officer Through a Close Reading of Digital Regulation and Policy,*" 20 July 2022, p. 2.
[41] Information Commissioner's Office listed fraud prevention and federated identity assurance services as examples of existing areas of data combination and matching application that requires data protection impact assessment. See ICO's "Examples of Processing 'Likely to Result in High Risk,'" available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/.
[42] In the US, law enforcement released a list of known online account usernames for a criminal who made sexual blackmail and death threats to more than 375 child victims (Buster Hernandez), which in turn enabled the identification of further potential offences on other platforms that would not be achievable without linking datasets across platforms. US Department of Justice (2021) "*Child Predator and Cyberterrorist, Buster Hernandez, aka "BrianKil," is Sentenced to 75 years in Federal Prison.*" https://www.justice.gov/usao-sdin/pr/child-predator-andcyberterrorist-.
buster-hernandez-aka-briankil-sentenced-75-years.
[43] The Wall Street Journal, Banks Start Using Information-Sharing Tools to Detect Financial Crime, 25 July 2023, available at https://www.wsj.com/articles/banks-start-using-information-sharing-tools-to-detect-financial-crime-11658741402.

- Research has shown that analysing criminal activities in massive multiplayer online games through cross-platform forensic investigations are hugely effective in combatting criminal activities online and identifying artefacts having evidential value for criminal investigations.[44]

The DMA makes all cross-use and data combination subject to user consent. On the member state level, the German Bundeskartellamt currently takes the view that "*general and indiscriminate data retention and processing across services without a specific cause as a preventive measure, including for security purposes, is not permissible [. . .] without giving users any choice*."[45] In other words, action could only be taken if a user has given consent in the case of the DMA or, in Germany, once a threat has materialised. However, such a delayed response is likely to render attempts at prevention meaningless.

CASE STUDIES OF DATA COMBINATION AND DATA CROSS-USE FOR SECURITY AND FRAUD PREVENTION

Identifying minors at risk of bad actors (e.g., groomers)

For example, companies may endeavour to proactively warn minors (email notifications) who might have been in contact with a child safety violator. Data combination and cross-use enable companies to provide these warnings cross-app, from, e.g., a video CPS to an email CPS.

Finding misrepresentations in age

Combination and cross-use enable companies to determine whether users might be misrepresenting their age on their apps/CPS. This not only helps companies ensure only people of age use their products but, more importantly, companies can use this as a signal to investigate

[44] Taylor DCPJ, Mwki H, Dehghantanha A, Akibini A, Choo KRR, Hammoudeh M and Parizi R, "F*orensic Investigation of Cross-platform Massively Multiplayer Online Games: Minecraft as a Case Study,*" page 5, Science and Justice, 2019.

[45] Bundeskartellamt, Statement of objections issued against Google's data processing terms, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html.

accounts where a person may pretend to be someone else on the other platform (for example, a groomer, pretending to be younger in order to contact minors on the company's (other) apps/CPS).

Ads/commercial content integrity

Combination and cross-use enable companies to determine and identify across their apps/CPS whether accounts are part of (network of) ad fraud, as well as to detect malicious behaviour through ads/commercial content so they can action these accounts after review.

Account Security

A common example: An attacker logs in to an account. There are certain suspicions based on the account metadata (e.g., IP, device, etc.), but the attacker has passed a login challenge (e.g., SMS verification, common when the mobile phone is stolen).

- The attacker changes the account recovery phone number (account data).
- The attacker then changes the billing information of the service.
- The combination of such a sequence of events and timestamps generally triggers confidence that a provider is dealing with an attacker and not a genuine user. At that point, decisive action is taken. None of this would have been possible without the cross-product data processing to verify.

Arguably, compliance with some of the obligations of the DSA might also be affected by Article 5(2) of the DMA. To be fully effective, threat detection, as required under Article 18 DSA, would likely also require cross-platform monitoring. Similarly, effective identification of a user repeatedly circumventing content moderation in accordance with Article 23 DSA would be aided by cross-platform monitoring. Finally, confirming the authenticity of an item of information as required by Article 35(k) DSA may also require checking across accounts on multiple platforms.

The co-legislators' intent with respect to the provision on data combination and cross-use was obviously to ensure that data driven-advantages cannot have the effect of substantially undermining the contestability of the core platform services. The GDPR recognises data security as a core principle in Article 5 (1) (f), whereas the DMA appears to treat it as an exception (see, for instance, Art. 6 (4) DMA). As the processing of personal data for data security and fraud prevention or safety-related processing across platform services seemingly does not have a direct relationship to that goal, such data processing then appears out of the DMA's scope.

To avoid legal uncertainty, it is imperative for the Commission, and other authorities seeking to regulate this area, to provide a clear definition of 'data combination' and 'cross-use of data' with a distinction to the already existing legal data protection framework of the GDPR. Specifically, any definition under the DMA would have to be limited to data processing falling into the scope of the DMA, leaving all others to the purview of the GDPR.

6 Limited Legal Basis Available for Data Combination or Cross-use of Data

As discussed above, the DMA allows for data combination or cross-use of data only, where either consent in the sense of Article 4, point (11), and Article 7 of the GDPR has been provided, or Articles 6(1), points (c), (d) or (e) GDPR are satisfied. However, the legal bases under the GDPR the DMA left untouched may not always be applicable for data combination or cross-data use specifically for purposes of data security and integrity and, e.g., prevention of criminal activities, which creates legal uncertainty for gatekeeper organisations.[46]

6.1 Legal Obligation, Vital Interest and Public Interest GDPR Grounds for Processing (Article 6(1), points (c), (d) or (e) GDPR)

The co-legislator was clearly aware of use cases of data combination and cross-use of data that do not impact the contestability of core platform services, as they allowed these practices for vital interest, public interest and legal obligation. However, no examples for use concrete cases are available, and these legal bases present an extremely high threshold to satisfy and will likely be unavailable for most use cases regarding safety, security and integrity.

The scope of Article 6(1) point (d) – vital interest, is limited to cases of concrete and imminent danger to the data subject or third persons,[47] and any preventative data security measures would often not qualify. [48]

Similarly, both the legal basis of "necessary for compliance with a legal obligation (Article 6(1)-point c) GDPR" and "necessary for the performance of a task carried out in the public interest" (Article 6(1)-point e) GDPR is of limited application in the context of data security or fraud prevention. Both require a clear basis established in Union or Member State law, and while certain national and EU legal

[46] Case C-77/21, *Digi Tavkozlesi es Szolgaltato Kft. V Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, 20 October 2022.
[47] *See*, Waltraut Kostchy "Article 6: Lawfulness of Processing," *in* Chistopher Kuner et al (org.), the EU General Data Protection Regulation: a Commentary (Oxford, Oxford University Press, 2020): 333.
[48] See, the WP29's Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, pp. 20 and 21.

instruments may require organisations to establish cybersecurity measures (i.e., NIS and the NIS2 Directive, and to a degree, the GDPR itself), their provisions would likely not meet the required legal standard.

Article 6(1)(c) of the GDPR does not provide explicit details on the specific types of legal obligations it encompasses; for a provision of EU law to be considered a "legal obligation" within the GDPR context, clarity and specificity are paramount.[49] For instance, Article 32 of GDPR mandates processors to establish suitable *technical and organisational measures, ensuring an adequate level of security*. However, the provision is not sufficiently clear and precise to use it as a reliable "necessary for compliance with a legal obligation" legal basis for personal data processing. Similarly, other EU legislation, such as the NIS2 or the Cybersecurity Act, does not establish a legal obligation that would necessitate personal data processing for data security or fraud prevention. More often than not, these legislations set a broad objective, leaving the specifics relatively undefined. As highlighted by the WP29, in such situations, a further specification may be required, enacted through secondary legislation or a binding decision by a public authority in a specific case.[50] In the case of DMA, the European Commission could potentially provide a more specific legal obligation for data security or fraud prevention through delegated acts.

Instead, outside the DMA, data combination and cross-use of data for data security and fraud prevention might often be covered by "legitimate interest" of Article 6(1)-point (f) GDPR. Recital 47 of the GDPR clearly states that *"the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."* The CJEU also appeared to consider system technical maintenance (including system testing and error detection) as an important and relevant activity in past judgments.[51]

Legitimate interest may also be the appropriate legal basis in cases where online service providers of any size may voluntarily support efforts of law enforcement in cases where consent is not an option and time is of the essence, such as search and recovery of individuals. The DMA, however, explicitly excludes legitimate interest as a possible legal basis for data combination in the scope of the DMA. Without further guidance, this leaves consent as the primary legal basis, which raises further questions.

---

[49] Ibid, 332.
[50] WP29 Opinion (2014), p. 20.
[51] Case C-77/21, *Digi Tavkozlesi es Szolgaltato Kft. V Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, 20 October 2022.

6.2 Consent

The DMA appears to introduce an apparent preference for consent as a legal basis for data combination and cross-use. This is contrary to the understanding that a hierarchy, at least among the legal bases GDPR provides, does not exist.[52]

In the case of the German Bundeskartellamt requiring a choice, also in the context of activities for data security and fraud prevention, this could ultimately mean expecting malicious actors to consent to the data processing to detect in advance the very malicious activity they intend to carry out.[53] Data security may also require the processing of personal data (such as IP addresses) beyond the user of a platform, who could technically be asked for consent (in the case of a firewall, for instance, which looks at the origin or destination of data including IP addresses as it controls access to a network). In general, data security is wider than interactions with end users, but certain other user groups (such as employees, for example) cannot be asked for consent, so the same data security measure may not have a consistent legal basis, depending on the user group.

Platforms below the gatekeeper threshold would, on the other hand, continue to have a wider array of legal basis at their disposal under the GDPR for fraud prevention or data security measures involving data combination or cross-use of data than gatekeeper platforms that hold arguably more data.

Additionally, some more practical questions arise:

- Where consent for data combination or cross-use of data that would now fall under the DMA was collected previously under the GDPR, there is a question of whether these would now have to be recollected for DMA compliance purposes. It is difficult to see how that would not be confusing to the end user.
- With respect to children's data in this context: is age verification required under the DMA (which would potentially mean additional data collection) and parental consent under the GDPR?
- How should consent withdrawal be managed in the context of the DMA? As a practical matter, data is not necessarily kept in separate silos inside companies, especially not when it comes to personal versus non-personal data.

[52] Article 5(2) of the Digital Markets Act.
[53] While rules under Articles 9 and 10 of the DMA allow for suspension or even exemption of certain obligations for Gatekeepers, they do not remedy any limitations with respect to data security, at least. They are exceptional in nature and, therefore, unlikely to be intended for regular everyday information security operations.

- From a user point of view, to the extent a user has enjoyed centralised controls (including over their privacy settings), separating data across services and products would force users to manage their accounts one by one. This would decrease the user experience and potentially lead to user confusion or inconsistencies across settings, contributing to the proliferation of consent.

Thus, more clarity regarding the relationship between DMA consent and the legal basis for the processing of personal data under GDPR is required. CIPL recommends the European Commission provide guidance to ensure that the processing of personal data that does not impact the contestability of the core platform services is not unnecessarily hindering the objectives of safety, security and integrity of gatekeeper services and of the wider ecosystem. Especially when it comes to data security measures, strictly necessary and proportionate measures should be possible without being tied to a consent requirement under DMA.

6.2.1 Consent Proliferation

As the DMA requires the separation of core services, users may expect an additional wave of consent requests, in addition to the numerous consent pop-ups already proffered on a daily basis, contributing to what is generally called consent or choice fatigue.[54]

If we also assume DMA consent for cross-service data use comes on top of potential existing GDPR consents, depending on how DMA consent is to be qualified, these additional consents will increase the requests users will face exponentially. For example, with three distinct GDPR consents that users can each individually accept or decline, users have eight different possible configuration options. If five separate consent options for cross-service data processing for five gatekeeper platform services are added to these GDPR consents that users can accept or decline individually, then users face a total of 256 different configuration options, among which they will have to choose. This, in addition to consent requests outside the DMA, becomes practically impossible for any individual to treat increasing consent requests as more than a mere box-ticking exercise.

[54] European Commissioner Didier Reynders announced a new initiative to tackle the growing concerns related to cookie fatigue. At the moment of writing this paper, the European Commission has not provided more details. D. Reynders' announcement can be accessed here:https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_2029.

Increasingly, we see also see more general questions being raised as to whether consent should be the standard of expressing one's informational self-determination in the digital ecosystem, exploring alternative ways for individuals to express their rights.[55]

6.3 Regulatory Cooperation

Finally, without more clearly structured regulatory cooperation as in the Dutch Digital Regulation Cooperation Platform[56] or the UK's Digital Regulator Cooperation Forum (DRCF), which also expressly includes the data protection authorities, there is a real danger of divergent interpretation over time of legal concepts defined under the GDPR such as consent, leading to legal uncertainty.[57]

At the moment of writing this paper, several Member States have published draft laws to implement DMA and to give their national competition authorities the power and competencies to conduct DMA investigations. The Dutch Government has published such an implementing act, which gives the ACM (Dutch Authority for Consumers and Markets) powers to conduct DMA investigations and, in some instances, exceed the powers given to the Commission. Crucially, the draft Dutch Act notes in its Article 2(1) that ACM is charged with monitoring compliance with Articles 5, 6 and 7 of the DMA. The national competition authority will seemingly be responsible for monitoring provisions related to the protection of personal data.

Cooperation mechanisms are of particular importance given Advocate General Athanasios Rantos' opinion,[58] which notes that competition authorities may, in the exercise of their powers, take account of the compatibility of commercial practice with the GDPR, and this assessment can only relate to incidental questions.[59] Furthermore, AG Rantos notes that in the absence of clear cooperation mechanisms, a competition authority has a duty to inform and cooperate with DPAs when interpreting GDPR.[60] Despite the existence of an obligation to cooperate, the absence of explicit and formalised cooperation mechanisms typically leads to a transparency deficit for regulated entities. Consequently,

---

[55] See Prof. Martin Nettesheim, EU Law Live No. 129, p. 6; CIPL will publish a separate paper investigating the user consent journey and its potential impact on the validity of consent.

[56] See https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt.

[57] For example, as reported by Politico on 12 April 2023, the French legislation to adapt national law to the DMA will go beyond the DMA and will be more strict in terms of its obligations.

[58] Opinion of Advocate General Rantos, Case C-252/21, 20 September 2022, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=265901&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=344793.

[59] Ibid, para 22.

[60] Ibid, para 29.

the formulation of such mechanisms becomes instrumental in fostering consistent enforcement of the law.

7 CONCLUSIONS

The main objective of the Digital Markets Act is to ensure fair and open digital markets by removing obstacles to the internal market in accordance with its own legal basis, and it should apply without prejudice to the GDPR. Yet the DMA limits the legal basis available under the GDPR for certain uses of personal data, i.e., data combination and cross-use of personal data in, Articles 5(2)(b) and 5(2)(c) DMA, respectively. As we have discussed above, it is in question to what extent the DMA can act as *lex specialis* to the GDPR and thus remove the certain otherwise available legal basis for specific processing activities. The interrelation between the DMA and the GDPR and how the scope of data protection provisions within the DMA should be interpreted, therefore, has to be further clarified. An argument can certainly be made that those data processing activities that do not have a link to the legislative intent of the DMA fall outside its scope and should, therefore, be possible under any applicable legal basis of the GDPR, including where these are data combination or cross-use of data. A clarification of what constitutes data combination or cross-data use in accordance with the DMA would provide the necessary legal clarity.