RSC 2023/68
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

WORKING PAPER

User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with ART. 5(2) DMA

Marco Botta and Danielle da Costa Leite Borges

European University Institute
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with ART. 5(2) DMA

Marco Botta and Danielle da Costa Leite Borge

RSC Working Paper 2023/68

ISSN 1028-3625

Published in December 2023 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy

With the support of the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Erik Jones, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The EUI and the RSC are not responsible for the opinion expressed by the author(s).

Centre for a Digital Society

The Centre for a Digital Society (CDS) was created in 2022 and is directed by Prof. Pier Luigi Parcu. It analyses the challenges of digital transformation and its impact on markets and democracy. Within the EUI, the CDS is part of the Robert Schuman Centre for Advanced Studies. With its research, policy debates and executive training programmes, the CDS aims to advise policy makers on how to cope with the challenges that are generated by the digitalisation process. To do so, it adopts an inter-disciplinary approach, relying on in-house expertise in law, economics and political sciences, and by actively cooperating with computer scientists and engineers from partner institutions. For further information: http://digitalsociety.eui.eu/

Abstract

The Digital Markets Act (DMA) is fully applicable since 2nd May 2023; the EU Commission has recently designated six firms having the status of 'digital gatekeepers' and thus subject to the DMA obligations. By imposing asymmetric regulation on 'large' digital platforms (i.e., gatekeepers), the new EU Regulation aims at improving the 'fairness' and 'contestability' of digital markets. In line with its goals, Art. 5(2) DMA prohibits gatekeepers from combining and cross using the end user's data collected from different sources within its own eco-system. However, Art. 5(2) DMA offers some exceptions to this general prohibition: data combination, in fact, is possible if the end-user provides his/her 'consent' to such data combination, to benefit from more personalized services/advertisement from the gatekeeper. In particular, the users' consent should comply with the requirements of Article 7 of the General Data Protection Regulation (GDPR).

The paper discusses the relationship between the DMA and the GDPR, focusing on the users' consent as a lawful basis to the processing activities of data combination and cross-use under Art. 5(2) DMA. The paper argues in favor of a 'privacy setting' solution, introduced by the gatekeeper within its platform service: at the first log in, the user would face on her/his screen a cookie wall, asking her/him to opt-in to specific types of data combination activities by the gatekeeper. Cookie walls have generally been considered not compatible with the GDPR requirement in terms of 'free' consent. However, in the online world, the emphasis on repeated, individual consent requests for every data processing has generated the so-called 'consent fatigue'. In the paper, we argue that the DMA anti-circumvention provision addresses the consent fatigue issue: in our view, if the gatekeeper had to ask for the user's consent every time before engaging in a data combination activity, this would represent a breach of Art. 13(6) DMA. Secondly, the paper argues that the DMA represents a lex specialis in comparison to the GDPR. Therefore, while respecting the general criteria indicated by Art. 7 GDPR, the user's consent under Art. 5(2) DMA should be 'adjusted' to the peculiarities of the Digital Markets Act.

Keywords

Digital Markets Act; General Data Protection Regulation; data combination; data cross-use; personal data; consent

Acknowledgements

The authors would like to thank Mario Viola, Antonio Manganelli, Maria Luisa Stasi, Oles Andriychuk, Kaja Breivik Furuseth, Heike Schweitzer, Isabella De Michelis, Marco Almada, Cristophe Carugati, Klaus Wiedemann, Friso Bostoen, Konstantina Bania, Giorgio Monti, Klaudia Majcher, Alba Ribera Martínez, Natalia Menéndez González and Viktoria Robertson for taking the time to read and comment a previous of this working paper. The authors are fully responsible for every error and mistake in the paper.

Table of contents

1. Introduction

The digital transformation has enabled the emergence of new business models, bringing to the front an economy based upon data processing power, storage, communication, and networks. In the last decade, digital platforms have been able to grow economically by collecting, accumulating, analysing, and delivering new personalised products and services.[1] The recognition of the increasing economic power of digital platforms' business model has resulted in new political responses, with a shift towards more governmental intervention *vis a vis* practices and business strategies of digital platforms.[2] In different parts of the world, we have thus been observing regulatory and legislative changes aiming at building a more comprehensive regulation of digital platforms' activities.[3]

The Digital Markets Act (DMA) represents the best example of the new sector regulation of digital platforms.[4] By imposing asymmetric regulation on 'large' digital platforms (i.e., gatekeepers), the DMA aims at improving the 'fairness' and 'contestability' of digital markets.[5] The 'digital gatekeepers' are platforms that provide at least one of the core platform services mentioned in the DMA,[6] and fulfil the DMA thresholds of application, in terms of number of users and turnover/market capitalization.[7] Platforms that fall within the scope of DMA application are required, within a period of 2 months, to notify their gatekeeper position to the EU Commission.[8] After having been officially designated by a EU Commission Decision, every gatekeeper is required to comply with the DMA obligations; in particular, 6 months after its designation, the gatekeeper should submit a report to the EU Commission, explaining the steps undertaken to comply with the DMA obligations.[9]

The DMA was adopted by the Council and by the European Parliament on 14th September 2022; it is fully applicable since 2nd May 2023.[10] On 6th September 2023, the EU Commission designated six firms as having 'gatekeeper' status, globally operating across eight core platform services that fall within the scope of the DMA application.[11] The designated gatekeepers will have to submit an auditing report about the status of the DMA implementation by March 2024. From that moment, the EU Commission will monitor the compliance by the gatekeepers with their obligations, eventually imposing fines,[12] as well as behavioural/structural remedies due to lack of compliance with the DMA obligations.[13] In addition, National Competition Authorities (NCAs) of the EU Member States will assist the EU Commission, by investigating cases of non-compliance within their own territory.[14]

1 Antonio Davola, Giancarlo Malgieri, "Data-Powerful. Un'Indagine sulla Nozione di Potere e il suo Rapporto con la Vulnerabilità nel Mercato Digitale'" Forthcoming in 2023 volume of *Concorrenza e Mercato.*

2 John Cioffi, Martin Kenney and John Zysman (2022), "Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century." 27(5) *New Political Economy:* 820-836.

3 Marco Botta (2021), "Sector Regulation of Digital Platforms in Europe: Uno, Nessuno e Centomila." 12(7) *Journal of European Competition Law and Practice:* 500-512.

4 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Act*). OJ L-265/1, 12.10.2022.

5 *Ibid,* Para 33-34 DMA Preamble.

6 Art. 2(2) DMA lists 10 "core platform services" that fall under the scope of application of the Regulation: online intermediation services, online search engines, social networks, video sharing platform, interpersonal communications services, operating systems, web browsers, virtual assistants, cloud computing and online advertising services. *Ibid.*

7 According to Art. 3 DMA, platforms providing at least one core platform service are presumed to have the status of gatekeeper when they have either a turnover of at least € 7.5 billion in the past 3 financial years or a market valuation of at least € 75 billion. In addition, a digital gatekeeper should have at least 45 million active end-users monthly, and at least 10.000 yearly active end users. *Ibid.*

8 *Ibid,* Art. 3(3) DMA.

9 *Ibid,* Art. 11 DMA.

10 *Ibid,* Art. 54 DMA.

11 Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft have been designated as digital gatekeepers by the EU Commission. In addition, the EU Commission has opened market investigations to determine whether Microsoft has gatekeeper status also in relation to Bing, Edge and Microsoft Advertising. The Commission has also opened market investigations Apple, to determine whether the firm has gatekeeper status also in relation iMessage and iPadOS. In accordance with the DMA, the EU Commission is required to conclude the market investigations within 12 months. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 (last access 8.11.2023).

12 The EU Commission may impose a fine up to 10% of the gatekeeper annual turnover in case of non-compliance with the DMA obligations. A further fine up to 20% of the gatekeeper turnover may be imposed by the EU Commission in case of repeated non-compliance by the gatekeeper. *Ibid,* Art. 30 DMA.

13 The EU Commission may impose on the gatekeeper "any" structural and behavioural remedy after having adopted 3 non-compliance decisions during the last 8 years. *Ibid,* Art. 18 DMA.

14 NCA may investigate cases of non-compliance with DMA obligations by gatekeepers within "its territory" and "subject to the powers defined by national law". While writing, a number of EU Member States (e.g., the Netherlands and Germany) are amending their

Finally, third parties (e.g., associations of consumers, business users and competing platforms) will be able to submit complaints both to the EU Commission and to NCAs about the gatekeeper's lack of compliance with the DMA obligations, as well as to start private enforcement actions in national civil and commercial courts.[15]

Art. 5(2) DMA prohibits a gatekeeper from combining and cross-using end users' data collected from different sources within its own eco-system.[16] However, Art. 5(2) DMA offers an exception to this general prohibition in case the end-user provides his/her 'consent' to such data combination and cross-use, to benefit from more personalized services/advertisement from the gatekeeper.[17] In particular, the users' consent should comply with the requirements of Article 7 of the General Data Protection Regulation (GDPR).[18]

Although Art. 5(2) falls under the DMA obligations that are considered 'self-executing',[19] its scope of application is far from being clear. In particular, the DMA does not clarify whether and to what extent the concept and requirements of 'consent' under the GDPR may be automatically applied to Art. 5(2) DMA, and thus whether any adjustment may be needed to this regard. The paper discusses the 'complex' relationship between the DMA and the GDPR, to clarify the scope of the user's consent to data combination under Art. 5(2) DMA. The paper first analyses the content of Art. 5(2) DMA. Secondly, the paper discusses the GDPR concept of consent and its requirements, in the light of the case law of the EU Court of Justice, as well as the guidelines adopted by the Working Party 29. Finally, the paper proposes a 'privacy-setting' solution that would allow the gatekeepers to comply with the requirements under Art. 5(2) DMA.

Several authors have extensively debated about the 'nature' of the Digital Markets Act – i.e., a hybrid legislation, inspired both by competition law and sector regulation of electronic communications.[20] On he other hand, the literature on the challenges faced by gatekeepers in terms of implementation of specific DMA obligations is still rather limited.[21] Similarly, several authors have analysed the concept of consent under the GDPR since this legislation was adopted in 2016.[22] By contrast,

national competition law in order to empower their NCA to investigate cases of non-compliance by the gatekeepers with the DMA obligations. *Ibid,* Art. 18 DMA.

15 Being an EU Regulation, the DMA is directly applicable in national court disputes between the gatekeeper and third parties. Damages requested, however, should be limited to non-compliance with the DMA obligations from the moment the platform has been designated as gatekeeper by the EU Commission Decision. Art. 42 DMA includes a reference to Directive 2020/1828, pointing out that a group of harmed consumers could start a representative action against the gatekeeper due to the collective damages caused by the breach of the DMA obligations. *Ibid,* Art. 42 DMA. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. OJ L-409/1, 4.12.2020.

16 *Ibid*.

17 *Ibid.*

18 Regulation (EU) 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L-119/1, 4.5.2016. Art. 7.

19 The EU Commission may adopt a Decision, specifying how each gatekeeper should implement, in practice, the obligations mentioned in Art. 6 and 7. By contrast, obligations falling under Art. 5 are considered self-executing, and thus the EU Commission is not expected to adopt any implementing act to this regard. *Supra,* Art. 8(2) DMA.

20 See, for instance: Natalia Moreno Belloso and Nicolas Petit (2023), "The EU Digital Markets Act (DMA). A Competition Hand in a Regulatory Glove." 48 *European Law Review:* 391; Anne Witt (2022), 'Platform Regulation in Europe—Per Se Rules to the Rescue?' 18(3) *Journal of Competition Law and Economics:* 670-708; Pinar Akman (2022), 'Regulating competition in digital platform markets: a critical assessment of the framework and approach of the EU Digital Markets Act' 47(1) *European Law Review:* 85-114; Oles Andriychuk, (2021) 'Shaping the New Modality of the Digital Markets: The Impact of the DSA/DMA Proposals on Inter-Platform Competition'. 44(3) *World Competition*: 261–286; Pierre Larouche, Alexandre De Streel (2021), 'The European Digital Markets Act: A Revolution Grounded on Traditions.' 12(7) *Journal of European Competition Law and Practice:* 542-560.

21 See, for instance: Alba Ribera Martínez, 'The Circularity of Consent In The Dma: A Close Look Into Articles 5(2) And 6(10).' Forthcoming in Autumn 2023 in *Concorrenza e Mercato;* Xingyu Yan, Huaiwen He (2022), 'Fine Tuning the *Ex-Ante* Approach to Data Combination Practices.' 18 *Journal of Competition Law and Economics:* 881-904; CIPL, *Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences*. Discussion paper published in April 2023. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf (last access 14.7.2023); Christina Etteldorf (2022), 'DMA - Digital Markets Act or Data Markets Act?' 8 *European Data Protection Law Review:* 255-261; Ief Daems (2022) 'The Complexity and Practical Challenges of Implementing the New DMA.' 7(2) *Competition Law & Policy Debate:* 106-112.

22 See, for instance: Elettra Bietti (2019), 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn.' 40(1) Pace Law Review: 307-397; Eleni Kosta (2020), 'Article 7. Conditions for Consent.' In Christopher Kuner, Lee A. Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR).* Oxford University Press.

limited attention has so far been devoted to the interaction between GDPR and DMA.[23] The paper aims at contributing to the on-going policy debate on the challenges faced by gatekeepers in the implementation of the DMA obligations; a topical subject after the entry into force of this Regulation. Secondly, the paper aims at contributing to the on-going debate on the relationship between DMA and GDPR.

2. DMA and the obligations for gatekeepers: Art. 5(2)

One of the competitive advantages enjoyed by a gatekeeper, in comparison to other platforms, is its ability to collect, combine and process end users' data from a variety of different sources within its own eco-system.[24] A gatekeeper can match the personal data provided by the end user when signing up for a digital service (e.g., signing up for a social network) with the 'traces' left by the end user while using the services provided by the gatekeeper within its own eco-system (e.g., web navigation history; apps downloaded; geo-location information; ads and videos watched…).[25] Thanks to data combination, the gatekeeper can 'profile' the end user, and it can thus provide more targeted services to the end user.[26] For instance, via profiling, the gatekeeper may automatically adjust the default app feature based on the user expected preferences. Similarly, the gatekeeper can provide a higher ranking to certain types of contents (e.g., specific videos, songs, apps, pictures, posts on social networks) that are considered 'more relevant' for the end user. On the other hand, the gatekeeper may also rely on data combination for target advertising and to carry out price discrimination:[27] Based on the end user behaviour within the eco-system, the gatekeeper may target the end user with specific ads and offers, which are considered (by the platform) to best match the end-users' interests and willingness to pay.

Personalized services/ads/prices should not be considered *per se* against the interests of end-users; several consumers enjoy more personalized offers and services, which decrease their searching costs.[28] However, users should be duly informed about data combination, and they should be able to freely provide their authorization (i.e., 'consent') to such use of their personal data. The GDPR requires the user's consent for 'data processing' – i.e., a broad expression that also includes 'data combination'.[29] However, consumers are often unaware that platforms collect and cross-use their personal data and they tend to accept the general terms and conditions provided by the platforms without fully understanding the effective scope of data combination within the platform eco-system. Secondly, data combination represents a major competitive advantage for gatekeepers in comparison to 'smaller' platforms, which provide a single service to consumers (e.g., via a single app and/or a website, rather than via an eco-system including different digital services), and thus they have a limited ability to engage in data combination activities.

The Digital Markets Act aims at fostering 'contestability' and 'fairness' of digital markets. According to its Preamble, 'contestability' is defined as "... the ability of undertakings to effectively overcome

23 See, for instance: Muhammed Demircan (2023), 'The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions'. In: Bieker, F., Meyer, J., Pape, S., Schiering, I., Weich, A. (eds) *Privacy and Identity Management. Privacy and Identity 2022*. IFIP Advances in Information and Communication Technology, vol 671. Springer, Cham. https://doi.org/10.1007/978-3-031-31971-6_12 (last access 14.7.2023); Inge Graef (2021), 'Why End-User Consent Cannot Keep Markets Contestable? A suggestion for strengthening the limits on personal data combination in the proposed Digital Markets Act'. *VerfBlog,* 2021/9/02, https://verfassungsblog.de/power-dsa-dma-08/ (last access 14.7.2023); Wolfgang Kerber (2022), 'Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law' 67(2) *Antitrust Bulletin*: 280-301; Anne Witt (2021), 'Data, Privacy and Competition Law.' *Graz Law Working Paper*, no. 24-2021.

24 Jan Krämer, Daniel Schnurr and Sally Broughton Micova, 'The Role of Data for Digital Markets Contestability', CERRE Report, September 2020. Available at https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/ (last access 12.7.2023). P. 55.

25 *Ibid*.

26 Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', WP 251 rev.01, 6 February 2018. Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (last access 12.7.2023).

27 Marco Botta, Klaus Wiedemann (2020), "To Discriminate or Not to Discriminate? Personalised Pricing in Online Markets as Exploitative Abuse of Dominance" 50 *European Journal of Law and Economics*: 381-404.

28 *Ibid*.

29 Under Art. 4(2) GDPR, "processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, …. alignment and combination…" *Supra*.

barriers to entry … and challenge the gatekeeper on the merits of their products and services."[30] The DMA thus aims at fostering both inter-platform competition (i.e. competition between the gatekeeper and other platforms operating in the contest of the same core platform service) as well as 'intra-platform' competition (i.e. competition between the gatekeeper and the business users that rely on the gatekeeper platform to provide their services to end users).[31] The DMA does not provide a definition of 'fairness', but rather 'unfairness'; the latter expression refers to "... an imbalance between the rights and obligations of the business users where the gatekeeper obtains a disproportionate advantage."[32] The DMA thus refers to 'fairness' in the contest of the Gatekeeper2Business Users relation, rather than in the contest of the Gatekeper2End Users relation. Therefore, in the contest of the DMA, fairness refers to intra-platform competition, by thus making rather unclear the distinction between the DMA contestability and fairness goals. Finally, the DMA Preamble also points out that fairness and contestability are 'intertwined', since "the lack of contestability … can enable a gatekeeper to engage in unfair practices",[33] by thus further blurring the distinction between fairness and contestability goals within the Digital Markets Act. As recently noticed by Colangelo, the EU legislator has not clarified the rationale of Art. 5 and 6 obligations; it is unclear whether each DMA obligation aims at achieving either the DMA contestability or fairness goal.[34] According to the author, most of the DMA obligations aim at achieving the DMA contestability goal, fostering primarily intra-platform competition.[35]

As mentioned in the previous section, Art. 5(2) prohibits a gatekeeper from combining personal data within its own eco-system in the lack of the user's consent. Art. 5(2) prohibition may be considered in line with the DMA 'contestability' goal: since the DMA obligations are applicable only *vis a vis* digital gatekeepers, third platforms will be able to continue combining and cross-using personal data, by thus improving their market position. At least in theory, Art. 5(2) should thus reduce one of the main competitive advantages enjoyed by gatekeepers, by thus fostering inter-platform competition.

It could also be argued that Art. 5(2) reflects the DMA fairness goal, remedying the current un-transparent way in which data combination is carried out by some gatekeepers. This is the interpretation recently followed by the Bundeskartellamt in its *Google* Decision adopted under Sec. 19(a) *Gesetz gegen Wettbewerbsbeschränkungen* (GWB).[36] Under Sec. 19(a)(2)(1)(4a) GWB, the Bundeskartellamt may prohibit a firm 'having paramount significance for competition across markets' from:

> "making the use of services conditional on the user agreeing to the processing of data from other services of the undertaking or a third-party provider without giving the user sufficient choice as to whether, how and for what purpose such data are processed."[37]

Both Sec. 19(a)(2)(1)(4a) GWB and Art. 5(2) DMA are applicable only to a selected number of 'large platforms' designed by the Bundeskartellamt and by the EU Commission. Although Sec. 19(a)(2)(1)(4a) is framed as a prohibition, while Art. 5(2) is an obligation for the gatekeeper, the content of the two provisions is rather similar: both provisions prohibit a 'large platform' from combining and cross-using personal data within its own eco-system without the users' consent. In its recent *Google* Decision,[38] the Bundeskartellamt has pointed out that Sec. 19(a)(2)(1)(4a) GWB "... concerns an

30 *Supra,* Para. 32 DMA Preamble.
31 *Supra,* Moreno Belloso and Petit (2023).
32 *Supra,* Para. 33 DMA Preamble.
33 *Supra,* Para. 34 DMA Preamble.
34 Giuseppe Colangelo (2023), 'In Fairness We (Should Not) Trust: The Duplicity of the EU Competition Policy Mantra in Digital Markets.' Pre-published online on the *Antitrust Bulletin*. The article is available at: https://journals.sagepub.com/doi/abs/10.1177/0003603X231200942 (last access 9.11.2023).
35 *Ibid.*
36 German Competition Act in the version published on 26 June 2013 (Bundesgesetzblatt (Federal Law Gazette) I, 2013, p. 1750, 3245), as last amended by Article 2 of the Act of 19 July 2022 (Federal Law Gazette I, p. 1214). An official English translation of the GWB is available at: https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0071 (last access 9.11.2023).
37 *Ibid,* Sec. 19(a)(2)(1)(4a) GWB.
38 Bundeskartellamt Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB, adopted in the administrative proceedings involving Alphabet Inc., Google Ireland Limited and Google Germany GmbH. Decision B7-70/21, adopted on 5.10.2023. The official English translation of the Decision is available at: https://www.bundeskartellamt.de/SharedDocs/Entschei-

exploitative conduct in the relationship between large digital companies and their users, which is regularly accompanied by the impediment of other companies."[39] According to the Bundeskartellamt, therefore, Sec. 19(a)(2)(1)(4a) primarily aims at safeguarding 'fairness' in the Platform2End Users relation, while 'contestability' considerations in the Platform2Business Users relation come at a second place. In other words, although the language of Sec. 19(a)(2)(1)(4a) prohibition is very similar to Art. 5(2) obligation, the first provision aims primarily at achieving a fairness goal, while the contestability goal guides the DMA obligation.

Art. 5(2) is the first of the 23 obligations included in the Digital Markets Act. The provision is framed as 4 'negative obligations' – i.e., the gatekeeper "shall not do any of the following". First, the gatekeeper shall not "process" personal data collected from third party apps and websites (e.g., newspapers and merchants' websites) together with the data collected within its own eco-system.[40] Secondly, the gatekeeper shall not "combine" personal data collected from different core platform services within its own ecosystem.[41] Thirdly, the gatekeeper shall not "cross-use" personal data collected within the core platform service with user's data collected from other services provided by the gatekeeper.[42] Finally, the gatekeeper shall not force end users to "sign in" end users to additional services, by thus forcing them to accept data combination requirements.[43] The four prohibitions may be considered, collectively, as a general prohibition on 'data combination' from the side of the gatekeeper.

Art. 5(2) provides four possible exceptions to the prohibitions mentioned above. First, the prohibitions are not applicable if the gatekeeper has provided a "specific choice" to the end user, and the latter has provided his/her "consent" to the data combination.[44] As further discussed in the following section, the consent should be expressed by the end user in accordance with the GDPR conditions for a valid consent.[45] Secondly, even in the absence of the user's consent, the gatekeeper may also combine/cross-use personal data in case the data processing is "necessary for compliance with a legal obligation to which the controller is subject."[46] Thirdly, data combination may take place without the user's consent if the latter is "necessary to protect the vital interests" of the end user.[47] Finally, data combination may be carried out by the gatekeeper, even in the lack of consent, in case it is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority" vested in the gatekeeper.[48]

In terms of enforcement, Art. 5(2) obligation will be applicable as soon as a platform is designed by the EU Commission as having the status of digital gatekeeper. As mentioned in the introduction, Art. 5 obligations are considered 'self-executing', and thus the EU Commission is not expected to adopt specific Decisions clarifying how each gatekeeper should comply with the data combination obligation.[49] Every gatekeeper, however, will have the burden of showing that it has duly complied with Art. 5(2), by providing a report to the EU Commission within 6 months after the gatekeeper designation.[50] In the report, the gatekeeper will have to specify the measures adopted to comply with the DMA obligations referring to the GDPR provisions, such as the user's consent under Art. 5(2) DMA.[51] In addition, the gatekeeper should also submit a report prepared by an independent auditor, explaining the profiling techniques applied by the gatekeeper *vis-à-vis* its end-users.[52] As pointed

dung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.html;jsessionid=117CE6482633DCFED42A25081F73765F.1_ci-d371?nn=3591568 (last access 9.11.2023).

39 *Ibid,* para. 42.
40 *Supra,* Art. 5(2)(a) DMA.
41 *Supra,* Art. 5(2)(b) DMA.
42 *Supra,* Art. 5(2)(c) DMA.
43 *Supra,* Art. 5(2)(d) DMA.
44 *Supra,* Art. 5(2) DMA.
45 Art. 5(2) DMA refers to the definition of 'consent' provided by Art. 4(11) and Art. 7 GDPR. *Supra.*
46 Art. 5(2) DMA refers to Art. 6(1)(c) GDPR, as possible legal basis for lawful data combination. *Supra.*
47 Art. 5(2) DMA refers to Art. 6(1)(d) GDPR, as possible legal basis for lawful data combination. *Supra.*
48 Art. 5(2) DMA refers to Art. 6(1)(e) GDPR, as possible legal basis for lawful data combination. *Supra.*
49 *Supra,* Art. 8(2) DMA.
50 *Supra,* Art. 11 DMA.
51 *Supra,* Para. 68 DMA Preamble.
52 *Supra,* Art. 15 DMA.

out by the DMA Preamble, such a report would aim at increasing the 'transparency' of the profiling techniques applied by gatekeepers *vis-à-vis* their end-users.[53] In particular, such a report would encourage the gatekeepers to "differentiate themselves (in comparison to other platforms) through the use of superior privacy guarantees".[54] The audit report thus aims at increasing the degree of competition between the gatekeeper and third platforms, relying on the DMA enhanced privacy protection standards as a new benchmark to assess the service quality provided by gatekeepers and third platforms. The auditor report will certainly have to explain the impact of the prohibition of the data combination obligation under Art. 5(2) with the ability by the gatekeeper to profile his/her users. Even so, the gatekeeper decided to continue to combine/cross-use personal data across its eco-system, by relying on the four exceptions provided under Art. 5(2), the auditor report should explain the impact (if any) of the reliance by the gatekeeper on such exception on its ability to profile end users.

3. Consent as a legal basis for data processing activities under the GDPR and the DMA

3.1. The relationship between DMA and the GDPR

Departing from the different terminology used by the GDPR and the DMA, which use respectively the terms "data subject" and "end user" to refer to the 'owners' of personal data processed by either the 'controllers' or the 'gatekeepers', these two pieces of EU law considerably differ in terms of objectives and scope. While the empowerment of data subjects in terms of strengthening control over their personal data is one of the main objectives pursued by the GDPR,[55] the DMA focus is on 'fairness' and 'contestability' in digital markets.[56] In other words, in the GDPR, the protection of natural persons and their fundamental rights and freedoms in relation to the protection of their personal data is the main and direct objective of the legislation, whereas in the DMA the protection of end users' personal data arises as an 'indirect objective' - or side-effect - connected to the obligations required from gatekeepers as a consequence of their data processing activities.

A second difference between the two legislations concerns the scope of data portability – i.e., the user/data subject right to ask the gatekeeper/data controller to transfer his/her personal data to a third party. Data portability is present both in the GDPR and in the DMA. In both legislations, the data controller/gatekeeper is required to share the data with third parties "free of charge."[57] Nevertheless, the scope of the two legislations is quite different. On the one hand, under Art. 20(2) GDPR, data portability is limited to 'personal data' that have been voluntarily and actively provided by data subjects to the controller.[58] On the other hand, within the DMA, data portability covers both 'personal' and 'non-personal data' generated by the end-user while using the core platform service.[59] Therefore, the DMA data portability obligation covers a wider range of data generated within the core platform service, such as raw data processed by connected devices, activity logs, web browsing history or web search activities. Finally, while the GDPR data portability is applicable only when it is "technically feasible",[60] the gatekeeper is requested to ensure "continuous and real-time access" to the data.[61] The DMA emphasis on "real-time access" shows a broader data portability obligation, in comparison to the limited scope of Art. 20 GDPR.[62]

53 *Supra,* Para. 72 DMA Preamble.
54 *Supra,* Para. 72 DMA Preamble.
55 *Supra,* Art. 1(1) GDPR.
56 *Supra,* Art. 1(1) DMA.
57 Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge." *Supra,* Art. 12(5) GDPR; *Supra,* Art. 6(9) DMA.
58 Jan Krämer (2020), 'Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations.' 17(2) *Journal of Competition Law and Economics:* 263-308.
59 *Supra,* Art. 6(9) DMA.
60 *Supra,* Art. 20(2) GDPR.
61 *Supra,* Art. 6(9) DMA.
62 Marco Botta (2023), "Shall we share? The principle of FRAND in B2B data sharing" EUI-RSCAS Working Paper 2023/30. P. 26. Available at: https://cadmus.eui.eu/handle/1814/75507 (last access 12.7.2023).

The different objectives and scope of the data portability right are good examples of the differences between the DMA and the GDPR. According to its Preamble, the Digital Markets Act is applicable "without prejudice" to the General Data Protection Regulation, as well as consumer and competition law.[63] As recently argued by Bania, the expression "without prejudice" means that the DMA obligations would be applicable without detriment to any existing right enshrined in the other legislations.[64] In line with this line of reasoning, you could conclude that the GDPR should always take precedence over the DMA in case of conflict between the two legislations.

Despite its reference to the expression "without prejudice", the DMA Preamble fails to clarify which legislation would prevail in case of conflict/divergent interpretation between the DMA and other sector legislation. By contrast, both the Data Act[65] and the Data Governance Act[66] stress the relevance of the GDPR in the interpretation of their provisions. The DMA and the GDPR are two EU Regulations: they have equal status within the hierarchy of EU legal norms. However, the two legislations have different objectives; even when dealing with the same issue (e.g., data portability), they follow rather different approaches. According to Bania, the DMA regulates a "more specific" subject than the GDPR, which is horizontally applicable to every type of data processing. Therefore, in view of the principle *lex specialis derogat generali,* in case of conflict between DMA and the GDPR, the first legislation should prevail.[67]

Alternatively, we could argue that the DMA and the GDPR are separate legislations that aim at achieving different objectives and follow different logics. When it comes to data combination, Art. 6(1) GDPR provide six possible legal bases for lawful data processing, including the data subject's consent. By contrast, Art. 5(2) provides only four possible legal bases to authorize data combination by the gatekeeper, including the user's consent. While designated gatekeepers will have to comply with Art. 5(2) requirement when carrying out data combination activities within their own eco-system, Art. 6(1) GDPR will be applicable to non-gatekeepers firms when they decide to combine, and thus process, collected personal data. To sum up, even without referring to the principle of *lex specialis,* we come to a similar conclusion: although the user's consent under Art. 5(2) DMA should be collected by the gatekeeper in light of the GDPR requirements for lawful consent, some adaptation would be needed in view of the GDPR peculiarities, since the two legislations are rather different in terms of objectives, logic and scope. Taking this important point in mind, the paper now turns to the analysis of the concept of consent according to the GDPR and DMA provisions.

3.2. Consent under the GDPR

The European Union model of data protection regulation is an example of how consent can be specifically regulated. Although the repealed Directive 95/46/EC already established consent as one of the lawful bases for the processing of personal data,[68] the General Data Protection Regulation introduced specific requirements on consent. Under Directive 95/46/EC, in fact, the data subject's consent meant "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[69] On the other hand, the GDPR in Article 4(11) establishes that:

63 *Supra,* Para. 12 DMA Preamble.

64 Konstantina Bania (2023), 'Fitting the Digital Markets Act in the Existing Legal framework: the Myth of the Without Prejudice Clause." 19(1) *European Competition Journal:* 116-149. At 117.

65 The Preamble of the Data Act proposal emphasizes that "this Regulation complements and is without prejudice to Union law on data protection and privacy, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications." Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM/2022/68 final. Preamble, para. 7.

66 The Preamble of the Data Governance Act emphasizes that "…this Regulation should not be read as creating a new legal basis for the processing of personal data for any of the regulated activities, or as amending the information requirements laid down in Regulation (EU) 2016/679." Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). OJ L-152/1, 3.6.2022. Preamble, para. 4.

67 *Supra,* Bania (2023), p. 148.

68 Art. 7(a) Directive 95/46/EC.

69 Art. 2(h) Directive 95/46/EC.

> "Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Therefore, the elements of consent are those enumerated in Article 4(11) GDPR. However, the GDPR also establishes 'conditions for consent' in its Article 7. In short, according to the latter provision, the elements of valid consent are the following: a) freely given; b) specific; c) informed; and d) unambiguous, with the indication of the of the data subject's will, given by a written or an oral statement according to which she/he agrees to the processing of her/his personal data.

The EDPB has provided further guidance on how to assess the elements for a valid consent.[70] According to its guidelines, in order for consent to be freely given, there must be real choice and control for data subjects.[71] Therefore, "[I]f consent is bundled up as a non-negotiable part of terms and conditions it is presumed to not have been freely given."[72]

Moreover, other issues must be considered when assessing whether consent is freely given. According to Recital 43 GDPR, when there is an imbalance of power between the data subject and the controller, consent should not be used as a legal basis for the processing of personal data, as it might prevent data subjects to exercise their free will. For instance, this can be the case when public authorities or employers are processing personal data concerning citizens and employees.

Another important issue for the assessment of freely given consent is 'conditionality'. In this regard, Recital 43 and Article 7(4) GDPR indicate that consent cannot be tied with the performance of a contract or the provision of a service. In other words, "consent and contract cannot be merged and blurred."[73] Hence, consent is not an adequate legal basis to the processing of personal data when the requested data is necessary for the performance of a contract. In this case, the adequate legal basis will be the one in Article 6(1) (b). On the other hand, if the personal data for which consent is sought is not necessary for the performance of a contract and its accomplishment is conditional on the data subject's consent, then consent is not considered to be freely given.

Therefore, there should always be a choice for the data subject to have either a contract performed, or a service delivered without having to consent to further data processing activities that are not essential for the performance of the contract in question. To avoid this type of 'conditionality', different contracts or services for data subjects must be proposed to data subjects by the provider or data controller: one including consent to the processing of personal data for further data processing purposes, and an alternative option, genuinely equivalent to the first contract or service offered by the same data controller, that does not contemplate consenting to additional data processing activities.[74] For instance, the EDPB when first assessing the requirements of consent, considered it to not be freely given when the controller uses 'cookie walls',[75] conditioning consent to the storing of data subject's information or to gaining access to information already stored in the data subject's device, as provided for in Article 5(3) of the ePrivacy Directive (Directive 2002/58/EC).[76]

70 EDPB (2020), Guidelines 05/2020 on consent under Regulation 2016/679. Adopted on May 2020. The document is available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (last access 13.7.2023).

71 *Ibid*, p. 7.

72 *Ibid,* p. 7.

73 *Ibid*., p. 10.

74 *Ibid*., p. 11.

75 A cookie is a small text file in alphanumeric format that is deposited on the Internet user's terminal or device (internet browser, computer etc.) by the server of the online service used (the website visited) or by a third-party server to track and identify users as they navigate the pages of a website. These files allow to recognize a visitor when he or she returns to the website, for instance, to remember products that the user has placed in his basket in a previous session. A 'cookie wall' designates the fact of conditioning access to a service on the acceptance by the Internet user of the deposit of cookies on her or his computer. The use of cookies is authorised by Article 5(3) of Directive 2002/58/EC (the "ePrivacy" Directive). See Commission Nationale pour la Protection des Données (CNPD) (2022) Le Règlement Général sur la Protection des Données: Lignes Directrices en Matière de Cookies et Autres Traceurs. Available at https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/cookies/CNPD-LD-Cookies.pdf> (last access 9.11.2023), p. 2-3.

76 *Supra*, EPDB guidelines 5/2020., p. 12.

In the same vein, the CJEU has also ruled in *Planet49* that the consent referred to in Article 6(1)(a) GDPR is not valid "if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent."[77]

This initial general ban on the use of 'cookie walls' for obtaining consent has been further developed by national courts and national data protection authorities leading to a more flexible approach to the use of 'cookie walls'. In this regard, in France, for example, the *Conseil d'État* by a decision from 19 June 2020, which discussed the French data protection authority (CNIL) guidelines on 'cookie walls' from 4 July 2019,[78] ruled that the requirement of free consent could not justify a general ban on the practice of 'cookie walls'.[79] According to this decision, the assessment of whether consent has been freely given must be done on a case-by-case basis, considering the existence of effective alternatives available to users in the event of refusal of cookies. In this specific ruling, however, the French Court concluded that the consent architecture used by Google for the creation of an account necessary for the use of the Android operating system provided only concise and very general information on the nature and purposes of the data processing activities carried out by Google ,and therefore could not be regarded as informed and consequently not valid.[80] In view of this ruling, CNIL reviewed its guidelines and recommendations on 'cookie walls'.[81] In 2022, CNIL has provided further guidance on how to assess the legality of the use of 'cookie walls', clarifying the criteria upon which the alternatives available to users to access websites without consenting to the processing of their data must be assessed. According to the 2022 CNIL guidelines, 1) web providers must make available to users 'a real and fair alternative' to walled content or services; 2) a paid alternative service must have a reasonable price; 3) user account creation must correspond to specific and transparent purposes; 4) paywalls and cookie walls must correspond to specific purposes; and 5) cookies may only be deposited in limited circumstances when an alternative to cookie walls is selected.[82]

Along the same lines, other data protection authorities have also issued guidelines on cookie walls in the last two years. This is the case of the Italian[83]and the Spanish[84] data protection authorities for instance. However, there are still national data protection authorities in the EU, such as the Belgian, which imposes a general ban on cookie walls arguing that they prevent obtaining free consent.[85]

This leads to the second important requirement for a valid consent: it must be 'specific'. This means that when consent is the chosen legal basis for data processing, it needs to be as granular as possible in order to be valid, making clear and specific to the data subject the purpose(s) for which consent is being sought. Therefore, if the data processing activity involves more than one purpose,

77 Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] ECLI:EU:C:2019:801. Para 44.

78 Commission nationale de l'informatique et des libertés (CNIL) (2019) Délibération n° 2019-093 du 4 juillet 2019. Available at https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038783337 (last access 24.7.2023).

79 Conseil d'État decision n° 430810 [2020] ECLI:FR:CECHR:2020:430810.20200619

80 *Ibid*, paras. 22 and 23.

81 Commission nationale de l'informatique et des libertés (CNIL) (2020) Délibération n° 2020-092 du 17 septembre 2020 portantadoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs » Available at: https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf (last access 24.7.2023).

82 Commission Nationale de l'Informatique et des Libertés (CNIL) (2022), Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL. Available at: https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/la-cnil-publie-des-premiers-criteres-devaluation and at https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ (last access 24.7.2023).

83 Garante per la Protezione dei Dati Personali (2021) Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876]. Available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876 (last access 24.7.2023). In section 6.1 II the Italian guidelines state that cookie walls are not considered a valid form of obtaining consent, except in cases in which the site owner offers the interested party the possibility of accessing an equivalent content or service without giving his consent to the installation and use of cookies or other tracking tools, to be verified however on a case-by-case basis.

84 Agencia Española de Protección de Datos (AEPD) (2023), Guía sobre el uso de las cookies. Available at: https://www.aepd.es/es/documento/guia-cookies.pdf (last access 24.7.2023). At p. 29, the Spanish guidelines state that "Web services may prevent users who do not consent to the use of cookies from access to the website or may offer a partial use of services, provided that users are adequately informed and that an alternative to the use of cookies is offered to the user, not necessarily for free, without need to accept the use of cookies. (authors' free translation).

85 See Autorité de protection des données - APD (2023) "Cookies et autres traceurs" Available at https://www.autoriteprotectiondonnees.be/professionnel/themes/cookies

all of them need to be specified and consented by the data subject. In other words, rather than bundling up all purposes in one, the data controller must seek several different consents from the data subject when there are different purposes for data processing activities.

The third essential requirement for consent to be valid is that it must be 'informed'. This is indeed part of the transparency principle that governs the GDPR. According to the EDPB, the minimum content requirements for consent to be informed comprise the following elements:[86] the controller's identity; the purpose of each of the processing operations for which consent is sought; what (type of) data will be collected and used; the existence of the right to withdraw consent; information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) GDPR where relevant; and on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46 GDPR.

In case the controllers do not comply with the minimum requirements for informed consent, this will be 'invalid', causing a possible breach of Article 6 of the GDPR. Furthermore, the general transparency requirements of Articles 13 and 14 of the GDPR should also be complied with when it comes to informed consent. In this regard, the Article 29 Working Party has clarified that when processing is based on consent (or explicit consent), information should include, for example, how consent may be withdrawn since it should be as easy for a data subject to withdraw consent as to give it according to Article 7(3) GDPR.[87]

The last essential requirement of consent concerns the unambiguous declaration of the data subject's will. In this regard, for consent to be valid it requires either a statement or a clear affirmative action from the data subject, who must consciously take action to consent to a certain data processing activity. According to Recital 32 GDPR, this deliberate action of consenting can take the form of a written or oral statement, by using recording and/or electronic means.[88]

Following up on *Planet49* ruling, the CJEU has further reiterated in *Orange Romania* the requirements for consent to be freely given and informed.[89] According to the Court, the burden is on the data controller to demonstrate that the data subject has, by an active behaviour, consented to the processing of her/his personal data.[90] This includes demonstrating that the data subject was informed, in an intelligible and easily accessible form, and in clear and plain language, that allows the data subject to understand the meaning and consequences of his/her consent. Moreover, the ruling clarifies that consent is not valid, for instance, for the collection and storage of IDs documents if it is included as a clause in a contract for the provision of telecommunications services which states that the data subject has been informed of, and has consented to, the collection and storage of their IDs, and where: i) the box referring to that clause has been ticked by the data controller before the contract was signed, or ii) the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or iii) the data subject's choice to object to the collection and storage is unduly affected by an additional form that they must fill to express their refusal to consent to those processing activities.[91]

Therefore, the GDPR provides for a more complex framework in relation to consent as one of the lawful bases to process personal data, though it is not the sole legal ground for the processing of personal data, nor hierarchically superior to the other legal bases, the use of consent should follow specific requirements in order to be considered adequate. In effect, in certain cases, obtaining consent may be inadequate and the controller must rely on the other lawful bases provided in Article 6 GDPR

86 *Supra*, EPDB guidelines 5/2020., p. 15.
87 Article 29 Working Party (2018) Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017 as last Revised and adopted on 10 April 2018.
88 *Supra*, EPDB guidelines 5/2020., p. 15., p. 18.
89 Case C-61/19, *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* [2020] ECLI:EU:C:2020:901.
90 Para. 52.
91 *Ibid*., para. 52.

for non-sensitive data or in Article 11 GDPR for sensitive data. Hence, consent is an appropriate legal basis in situations where serious data protection risks emerge, requiring, consequently, a high level of choice and control from data subjects over how their data are used.[92]

The paper moves now to the analysis of the use of consent as a lawful legal basis for the data processing activities provided for in Art. 5(2) DMA.

3.3. Consent under Art. 5(2) DMA - a Privacy-Setting Solution

As discussed in section 2, Art. 5(2) DMA prohibits the gatekeeper from combining and cross-use the user's data collected within its own eco-system. However, data combination is possible in case the end user has provided his/her consent, in accordance with the GDPR requirements. Article 5(2) DMA, in fact, explicitly defines 'consent' "within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679."

As discussed in the previous section, the GDPR gives a special protection to consent as an appropriate legal basis in situations where serious data protection risks emerge, considering the high level of choice and control that it requires from data subjects. However, the power imbalance present in the relationship between end users/data subjects and gatekeepers (digital online platforms) may end up in converting the granting of consent under the DMA a difficult task, considering all the requirements connected to consent established by the GDPR: the consent should be freely given; specific; informed; and unambiguous.

As a preliminary point, we should discuss whether and to what extent the relationship between the user and the gatekeeper is *per se* 'imbalanced' within the meaning of Recital 43 GDPR, and thus the user's consent to data combination would be *per se* invalid. Ribera Martinez has recently defined this issue as the 'circularity problem' between the concept of consent under the DMA and the GDPR.[93] In its recent ruling in the *German Facebook* case, the EU Court of Justice has pointed out that, even if the data controller is a dominant online platform, this does not make *per se* the data subject's consent invalid.[94] According to the CJEU, the consent validity should be assessed on a case by case basis, in relation to the degree of effective freedom enjoyed by the online user to reject a specific request of data processing, rather than linked to the dominant position of the platform.[95] Although the *German Facebook* ruling concerns a competition law case, the CJEU interpretation could be applied *mutatis mutandis* to the concept of consent under Art. 5(2) DMA. Such interpretation is also supported by a literal interpretation of Art. 5(2) DMA, which explicitly grants to the gatekeeper the possibility to continue its data combination/cross-use activities after having collected the user's consent.

It is worth pointing out that the DMA Preamble has further specified the scope of the consent exception provided in Art. 5(2). First, the 'specific choice' requirement implies that the gatekeeper should provide to the end user "to freely opt-in" to such data combination,[96] especially via a "user-friendly solution."[97] Therefore, the gatekeeper should not force the end user to provide his/her consent to the data combination. For instance, the gatekeeper could not threaten the end user that the service would not be provided anymore in the lack of consent to data combination. Secondly, when collecting the consent, the gatekeeper should provide to the end user a choice between a more personalized service, resulting from providing consent to the data combination, and a "less personalised but equivalent alternative."[98] The DMA Preamble points out that the "less personalised alternative should not be different or of degraded quality compared to the service provided to end

92 *Supra,* EPDB guidelines 5/2020, p. 20.
93 *Supra,* Ribera Martinez.
94 Case C-252/21, *Meta Platforms v. Bundeskartellamt* [2023] ECLI:EU:C:2023:537. Para. 147.
95 *Ibid,* para. 150.
96 *Supra,* Para. 36 DMA Preamble.
97 *Supra,* Para. 37 DMA Preamble.
98 *Supra,* Para. 36 DMA Preamble.

users who provide consent."[99] Thirdly, at the time of collecting the consent on the data combination, the gatekeeper should inform the end user about the features of the "less personalised offer" resulting from not providing the consent.[100] Finally, the end user should always remain free to either modify or withdraw its consent to data combination at any time.[101]

From a theoretical perspective, providing a "less personalised service" implies that the service features provided by the gatekeeper may not be influenced by the consent to data combination; only the 'user experience', when navigating the platform/service, may be affected by the lack of data combination. From a practical perspective, it is quite hard to imagine how the gatekeeper could provide a "less personalized but equivalent" service: personalization is the main added value of the services provided by a gatekeeper in comparison to competing platforms, which have access to a ower variety of data, and thus they can provide only 'less personalized' services. In the digital world, service 'personalization' and 'quality' are often intertwined concepts. Making a digital service 'less personalized' while keeping the same quality is one of the main challenges that the gatekeepers will have to face in the contest of the compliance with Art. 5(2) requirements.

The concept of consent is thus well established under the DMA Preamble. On the other hand, the DMA does not provide for indications on the architecture design of consent by the gatekeeper. This might open the door for different experiments that could hinder the capacity of users to fully exercise their free choice and their capacity of granting consent in an informed, specific, and unambiguous manner. In particular, the problem might rise by the fact that Art. 5(2) DMA is, in theory, a self-executing obligation – i.e., the EU Commission is not expected to adopt a separate Decision to clarify how each gatekeeper should in practice collect the users' consent under Art. 5(2). This uncertainty also opens the door for future legal disputes around the appropriate architecture design of consent.

In view of the DMA Preamble requirements and considering the consent conditions under Art. 7 GDPR, we could argue that the gatekeeper could design a specific 'privacy setting' tool within its platform service to collect the users' consent to data combination and cross-use. In line with the DMA Preamble, the data combination consent should be based on a freely opt-in system, designed in an understandable manner for the user (i.e., non-technical language). In other words, the user should be fully aware that, by authorizing the gatekeeper to carry out data combination and cross-use activities, he/she will receive a personalised service, as well as he/she will be subject to target advertising. On the other hand, in case the user decided to opt out from data combination, he/she would receive a 'less personalised' service, as well as general advertising. Since several gatekeepers deliver 'free' online service to their users thanks to the revenues generated by target advertising, opting out from the data combination might also imply that the gatekeeper could ask the user for monetary compensation to continue using the service.[102] Although this possibility is not explicitly mentioned in the DMA preamble, this interpretation is supported by the recent *German Facebook* ruling. In the judgment, the CJEU has pointed out that the online user should never be forced by the dominant online platform to grant his/her consent to a specific data processing activity.[103] However, in case of consent refusal, the platform should grant to the user the possibility to continue using the service subject to "an appropriate fee."[104]

In our view, the privacy-setting solution would guarantee that the consent provided by the user is 'freely given', 'specific', 'informed' and 'unambiguous', in accordance with Art. 7 GDPR. To be 'specific', the privacy setting solution should not include a general opt-in, granting to the gatekeeper

99 *Supra,* Para. 37 DMA Preamble.

100 *Supra,* Para. 37 DMA Preamble.

101 *Supra,* Para. 37 DMA Preamble.

102 In effect, since November Meta has started to offer its Facebook and Instagram users in Europe the option to pay for an ad-free version. The prices of this ad-free version ranges from 10 to 13 EUR depending on the system used (IOS or Android). The ad-supported version of the services will continue to be available under the consent requirement. According to Meta, the ad-free paid version "balances the requirements of European regulators while giving users choice and allowing Meta to continue serving all people." (as cited by The Associated Press in the article "Meta rolls out paid ad-free option for European Facebook and Insta users after privacy ruling" (October 30, 2023) Available at: https://apnews.com/article/facebook-instagram-meta-europe-ads-privacy-09c2bf513b819d-77c43884e3b84a79e5 (last access 9.11.2023).

103 *Supra,* case C-252/21, para. 150.

104 *Supra,* case C-252/21, para. 150.

a 'free cheque' in terms of different typologies of data combination. The new platform setting should include a 'granular' list of data combination activities carried out by the gatekeeper; the user should be free to select which types of data combination activities to opt in. Finally, the user should be free to modify the settings at any time, in terms of opting-in and out to/from specific data combination activities, and by withdrawing consent.

As a practical example of the privacy-setting solution, Facebook could ask its users whether they would like to authorize Meta to combine their personal data collected from the Facebook platform with their profile's activities on WhatsApp and Instagram. Similarly, Facebook would ask its users whether they would like to authorize Meta to combine their profile data with their personal data collected from third parties (e.g. apps and web-sites visited by the users). Each type of data combination would be subject to a separate opt-in consent (i.e. 'granular list' of consents); at any time, the user could modify/withdraw the consent for any specific type of data combination. The consent, however, would only cover data combination and data cross-use within the platform eco-system; data processing in general, by contrast, would fall outside of Art. 5(2) DMA and thus it would continue to be regulated under the Art. 6 GDPR legal bases. In addition, consent under Art. 5(2) DMA would only cover data combination activities carried out by the gatekeeper among different core platform services. As further discussed in the following pages, services not designated by the EU Commission Decision do not fall under the scope of Art. 5(2) DMA, while they might be subject to a separate decision by the Bundeskartellamt under Sec. 19(a) GWB, as in the recent Google commitment decision.

A critical point to discuss concerns the 'number of times' in which the gatekeeper should ask for consent to data combination from its user. As argued in the previous section, some Data Protection Authorities in Europe (e.g. Belgium DPA) and the CJEU case law have generally considered cookie walls as incompatible with the requirement of consent under Art. 7 GDPR. Some Data Protection Authorities, in fact, have emphasized that the data subject should provide his/her consent to every processing of his/her personal data. In the online world, the emphasis on 'individual' consent to data processing has caused the so-called 'consent fatigue'.[105] The latter expression refers to the situation where the data subject is repeatedly asked to provide his/her consent to a specific type of data procession. Although the data subject might initially decide to deny his/her consent, in the long term, due to the repeated requests and the complexity of the privacy terms, he/she might finally grant the consent, by thus nullifying the user's decision-making autonomy. The consent fatigue may be considered one of the 'side effects' of the GDPR, which requires the data subject to provide his/her consent to every data processing. Consent fatigue is often referred to as the emotional effects caused by the overload of too many consent requests that may create a state of mind in individuals capable of watering down the real choice implied in consent.[106]

To prevent consent fatigue, Art. 5(2) provides that, in case the end user has either refused/withdrawn his/her consent, the gatekeeper should not repeat the consent request "more than once within a period of one year."[107] In addition, a repeated request of the user's consent by the gatekeeper could also be considered a breach of the DMA anti-circumvention rule. According to Art. 13(6) DMA, in fact, the gatekeeper should not make the exercise of the rights provided by the DMA to end users "unduly difficult", in particular "…by subverting end users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface."[108] Generally speaking, Art. 13(6) DMA sanctions the so-called 'dark patterns' – i.e., deceptive online practices that mislead consumers, pushing them to specific types of unwanted behaviours.[109] The classical example of dark

105 Thomas Wein (2022), 'Data Protection, Cookie Consent and Price.' 10(12) *Economies:* 307-336.

106 Schermer, B.W., Custers, B. & van der Hof, S. (2014), 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection'. 16 *Ethics Inf Technol*: 171–182.

107 *Supra,* Art. 5(2) DMA.

108 *Supra,* Art. 13(6) DMA.

109 In relation to dark patterns in the online world, see: Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' Forthcoming in Ramsi A. Woodcock, *Toward an Inframarginal Revolution: Markets as Wealth Distributors,* Cambridge University Press 2023. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4411537 (last access 14.7.2023); Jamie Luguri and Lior Jacob Strahilevitz (2021), 'Shining a Light on Dark Patterns.' 13(1) *Journal of Legal Analysis:* 43-109; Midas Nouwens and others (2020), 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence.' Conference paper presented at the 20 CHI Conference on Human Factors in Computing Systems, April 25-30, 2020,

pattern is when an online intermediation platform creates a time pressure on an end user to conclude an online purchase, claiming that the product price will increase if the purchase is not concluded within a limited period of time. Such a time pressure reduces the ability of the consumer to compare different online offers, and thus it limits the consumer's decision-making autonomy. It could be argued that repeated consent requests to data processing, common in the online world, may also be considered as 'dark patterns' that limit the user's decision-making autonomy. Therefore, a repeated consent request by the gatekeeper to authorize data combination may be considered both in breach of Art. 5(2) DMA, as well as a breach of the anti-circumvention rule under Art. 13(6) DMA.

In view of these considerations, we could argue that consent under Art. 5(2) DMA should be 'adjusted' to the peculiarities of the Digital Markets Act. In view of Art. 13(6) DMA, the privacy setting solution discussed above could be designed as a cookie wall, popping up on the user's screen at the first log into the platform service after the gatekeeper implements Art. 5(2) obligation, and thus introduces the new privacy setting. The user would thus be required only once by the gatekeeper to adjust the privacy setting of the platform service, by opting in and out for different types of data combination and cross-use. The settings defined by the user at the first log in would remain in place, without the need for the gatekeeper to collect the user consent every time he/she access the platform service. In case the gatekeeper decides to introduce new types of data combination and cross-use within its own eco-system, the user should be informed and he/should be asked whether he/she would like to opt-in. Finally, as mentioned above, the user could always modify the privacy settings of the platform service, by opting in and out for specific typologies of data combination and cross-use.

The privacy setting-solution would represent an 'adjustment' of the concept of consent in the GDPR to the peculiarities of the Digital Markets Act, complying at the same time with all the consent requirements set out by the GDPR - and its interpretation by data protection authorities, EDPB, national courts and the CJEU – as previously discussed in Section 3.2. Such an adjustment would be possible because, as argued above, the DMA may be considered a *lex specialis* in comparison to the GDPR. Secondly, the privacy-settings solution would be in line with Art. 13(6) DMA and would prevent the consent fatigue that has characterized the GDPR enforcement in the online world.

3.4. The German Meta and Google cases: the first attempts to comply with the new data combination requirements

It remains to be seen whether and to what extent individual gatekeepers will introduce a privacy setting solution to comply with Art. 5(2) DMA. One of the first examples to this regard is the accounts centre, recently announced by Meta as a commitment in the contest of the *German Facebook* case. [110] According to Meta's proposal, its users:

> "for the first time will be able to make a largely free and informed decision about whether they want to use Meta's services separately or in combined form. Using the services in combined form would allow them to use additional functionalities such as cross posting, where a post is simultaneously published across several social media outlets, but Meta would then use the combined data for advertising purposes."[111]

Although Meta has introduced the accounts centre to comply with the 2019 *Bundeskartellamt* antitrust decision, the solution could be applied *mutatis mutandis* by Meta to comply with Art. 5(2) DMA. This solution looks like that of consent management platforms, currently used by several websites to implement cookie consent interfaces to obtain users' permission to use non-essential cookies. These platforms, also known as Consent Management Providers (CMPs), offer consent pop-

Honolulu. Paper available at: https://people.csail.mit.edu/ilaria/papers/Midas-MITCHI2020.pdf (last access 14.7.2023).

110 Bundeskartellamt (2023) Meta (Facebook) introduces new accounts center – an important step in the implementation of the Bundeskartellamt's decision. Press release, 7 June 2023. Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_Meta_Daten.html;jsessionid=5043FBA1D762A17CBB84CC1B45F27C9A.1_cid371?nn=3591568 (Last access 13.7.2023).

111 *Ibid*.

ups that are embedded in websites to enable streamlined compliance with the legal requirements for consent.[112] If gatekeepers opt to use this kind of privacy setting, outsourcing this consent management to a third party, they will need to clearly define the role of CMPs as processors - with the meaning of Article 4(8) GDPR. The CMPs, in fact, will be processing personal data on behalf of gatekeepers. In this case, a contract meeting the conditions of Article 28 GDPR should be concluded between the gatekeepers and the company offering the consent management platform.[113]

Another interesting development is represented by the recent Bundeskartellamt decision in the *German Google* case. In October 2023, the Bundeskartellamt accepted the commitments offered by Google in the contest of the investigations opened under Sec. 19(a)(2(1)(4a) GWB - i.e. the equivalent provision to Art. 5(2) DMA.[114] In particular, Google committed not to combine and cross-use personal data collected among its different digital services as well as via third-party web-sites.[115] While Art. 5(2) DMA is applicable only to the Google 8 core platform services, designated by the EU Commission as having gatekeeper status in September 2023, the Bundeskartellamt decision covers the remaining services provided by Google.[116] For example, Google Android Auto, Google Photos and Google TV have, for the moment, not been designated as having gatekeeper status by the EU Commission under the DMA; therefore, Google could continue to combine and cross-use these data without the users' consent. However, these services are now covered by the scope of the Bundeskartellamt decision. The commitments offered in the contest of the *German Google* case would be applicable only to the services not designated by the EU Commission under the DMA.[117] Although the commitments bind Google only in relation to its business activities in Germany,[118] *de facto* the commitments broaden the scope of the data combination obligation under Art. 5(2) DMA. In fact, it would be too costly, and thus rather unlikely, for Google to comply with the Bundeskartellamt decision only in relation to Germany, and not for the other EU Member States. Therefore, the Bundeskartellamt decision has *de facto* extended Art. 5(2) obligation to the entire Google eco-system across the entire European Union.

In accordance with the commitments accepted by the Bundeskartellamt, Google should provide both registered and non-registered users a specific choice not only to authorize data combination across its services, but also to explicitly 'decline'' it.[119] Secondly, Google should provide a 'transparent' to its users:[120] Google should explain to its users whether to what extent cross-service data processing would take place even in the lack of the users' consent; the choice option should be set up in a clear way, both in a 'technical and visual manner'; the users should understand how the consent options for the different types of data combination activities relate to each other; last but not least, the choice options should be phrased 'objectively'. In spite of its different scope of application in comparison to Art. 5(2) DMA, the commitments accepted by the Bundeskartellamt in the *German Google* represent a useful example of how gatekeepers could comply in the future with Art. 5(2) obligation. The commitments closely follow the privacy-setting solution advocated in the previous pages.

112 Santos, C., Nouwens, M., Toth, M., Bielova, N., Roca, V. (2021), 'Consent Management Platforms Under the GDPR: Processors and/or Controllers?'. In: Gruschka, N., Antunes, L.F.C., Rannenberg, K., Drogkaris, P. (eds) *Privacy Technologies and Policy*. APF 2021. Lecture Notes in Computer Science(), vol 12703. Springer, Cham.

113 Commission Nationale por la Protection des Données (CNPD) (2022) "Le Règlement Général sur la Protection des Données: Lignes directrices en matière de cookies et autres traceurs", p. 18. Available at: https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/cookies/CNPD-LD-Cookies.pdf (last access 24.7.2023).

114 *Supra*, Bundeskartellamt decision in case B7-70/21.

115 *Supra,* Bundeskartellamt decision in case B7-70/21, para. 62.

116 The Commission DMA designation decision adopted on 6th September 2023 covers the services provided by Google: Google Shopping, Google Play, Google Maps, YouTube, Google Search, Chrome, Google Ads, Chrome. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 (last access 9.11.2023).

The commitment decision adopted by the Bundeskartellamt in the German Google case covers the following services provided by Google: Accommodations, Assistant, Android Auto, Android Automotive, Android TV, Authenticator, Calculator, Chrome WebStore, Clock, Contacts, Files by Google, Flights, Gallery Go, Gboard, Google One, Google Photos, Google Sign-In, Google TV, Jobs, News, Translate, Wallet, Workspace Communications, Workspace Document Processing, Workspace Email & Scheduling. *Supra,* Bundeskartellamt decision in case B7-70/21. Annex.

117 The commitment decision specify that when a service provided by Google is designed by the EU Commission under the DMA, Art. 5(2) DMA replaces the offered commitments. *Supra,* Bundeskartellamt decision in case B7-70/21. Annex - Commitments Offer pursuant to Sec. 32b GWB, section B.III.

118 *Supra*, Bundeskartellamt decision in case B7-70/21, para. 69.

119 *Supra,* Bundeskartellamt decision in case B7-70/21. Annex - Commitments Offer pursuant to Sec. 32b GWB, section B.I.1.

120 *Supra,* Bundeskartellamt decision in case B7-70/21. Annex - Commitments Offer pursuant to Sec. 32b GWB, section B.II.5.

The accounts centre recently introduced by Meta and the commitments recently accepted by the Bundeskartellamt in the contest of the *German Google* case are the first examples of how gatekeepers could comply with Art. 5(2) obligation. These solutions would allow gatekeepers to continue combining personal data collected within their eco-system, while complying both with the DMA and the GDPR requirements. It remains to be seen, however, whether and to what extent other designated gatekeepers will follow a similar approach to comply with Art. 5(2) DMA and how the EU Commission will assess the compatibility of these solutions with Art. 5(2) DMA.

4. Possible justifications and alternative legal bases for data combination activities under Art. 5(2) DMA

4.1. Alternative legal bases to authorize data combination under Art. 5(2) DMA

In addition to collecting the user's consent, Art. 5(2) DMA provides three additional legal bases to allow the gatekeeper to combine data within its own eco-system. According to Article 5(2), in fact, gatekeepers can rely only on the following legal basis provided by Article 6(1) GDPR: point (c) compliance with a legal obligation to which the controller is subject; point (d) to protect the vital interests of the data subject or of another natural person; and point (e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

It is worth to be notice that the gatekeeper cannot rely on legal bases provided by Article 6(1), points (b) and (f) GDPR to justify the combination of data under Art. 5(2) DMA.[121] Art. 5(2) thus includes a 'shorter' list of legal bases for data combination in comparison to the list of legal bases for lawful data processing under Art. 6 GDPR. Secondly, the legal bases mentioned by Art. 5(2) DMA have a 'stricter' application according to GDPR, and their interpretation by data protection authorities, the EDPB and the CJEU. In relation to Article 6(1)(c) (i.e., controller process the personal data to comply with a legal obligation), Article 6 (3) GDPR elucidates that this legal basis can be used only where a processing operation is imposed on an organisation by EU or national legislation. The EDPB has clarified other conditions that must be met for the lawful processing under Article 6(1)(c). It considers that the legal provisions must establish a clear and specific obligation to process personal data; these legal provisions must at least define the purposes of the processing; and the obligation to process data should be imposed on the controller and not on the data subjects. In case these conditions are not met, the processing activities cannot rely on Article 6(1)(c), and thus another legal basis must be sought by the controller.[122] Examples of processing activities that can rely on Article 6(1)(c) are employers that need to process their employees' personal data for social security purposes, or businesses that need to process their clients' or customers' personal data for tax purposes.[123] The application of Art. 6(1)(c) GDPR was also recently discussed by the CJEU in the *German Facebook* case. In the ruling, the CJEU concluded that it is for the German national court to inquire whether Meta Platforms Ireland is under a legal obligation to collect and store personal data in a preventive manner in order to be able to respond to any request from a national authority seeking to obtain certain data relating to its users, and consequently to rely on Article 6(1)(c) GDPR.[124]

Regarding the use of Article 6(1)(d) as a legal basis (i.e., data processing is necessary to protect the vital interests of the data subject), the GDPR states in Recital 46 that the use of this legal provision for lawful processing "in principle take place only where the processing cannot be manifestly based on another legal basis." Furthermore, this Recital also illustrates some situations by which processing may serve both important grounds of public interest and the vital interests of data subjects, such as

121 Art. 6(1), points (b) and (f) GDPR refer to the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; and purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

122 EDPB (2023) "Data protection guide for small business", Section 'Process personal data lawfully: Compliance with a legal obligation of the controller'. Available at: https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en (last access 24.7.2023).

123 *Ibid.*

124 Supra, Case C-252/21. Paras. 29 and 137. Para 132.

the monitoring of epidemics and humanitarian emergencies, "in particular in situations of natural and man-made disasters."[125] The UK Information Commissioner's Office (ICO) guidelines, for example, explain that due to its limited scope, Article 6(1)(d) will only apply to life and death situations, such as emergency medical care, when the processing of personal data is necessary medical treatment purposes but the individual is incapable of giving her/his consent due to life-threatening injuries.[126] Along the same lines, the CJEU concluded in the *German Facebook* ruling that a social network such as Meta, whose activity is essentially economic and commercial in nature, cannot rely on Article 6(1) point (d) of the GDPR to justify the processing of personal data of their users without their consent on the basis of the general terms in force.[127]

Finally, when it comes to the application of Article 6(1)(e) (i.e., controller should process the data either in the public interest or to carry out a public interest function), Recital 45 GDPR and Article 6(3) state that to rely on this legal basis the processing should be based on EU or national law, and that the processing must be proportionate to the legitimate aim pursued. Moreover, Recital 45 further develops that it is for Union or national law to determine whether

> "the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association."[128]

In this regard, the CJEU in the *German Facebook* ruling concluded that it is for the German national court to determine whether Meta Platforms Ireland was entrusted with a task carried out in the public interest or in the exercise of official authority, when carrying out research for the social good and to promote safety, integrity and security. However, the Court emphasised that given the type of activity and the economic and commercial nature of the company, "it seems unlikely that a private operator was entrusted with such a task."[129] Furthermore, the CJEU also stressed that considering the scale of the data processing activities carried out by Meta Platforms Ireland and of its significant incidence on the users of the social network Facebook, the referring court should also determine whether the processing activities were strictly necessary.[130]

The EDPB illustrates, for instance, that organisations exercising medical practice and processing general practitioners' personal data to ensure that their qualifications, moral and ethical conduct meet the standards set in the country where the organisation is located can rely on Article 6(1)(e) for processing activities.[131] ICO in turn exemplifies the use of this legal basis by private water companies when carrying out functions of public administration and exercising special legal powers to carry out utility services in the public interest.[132]

To sum up, Art. 5(2) DMA provides for three 'alternative' legal bases that the gatekeeper could rely upon to combine personal data within its eco-system without collecting the user's consent. However, the legal bases mentioned in Art. 6(1)(c)(d)(e) GDPR have been 'strictly' interpreted by the CJEU and by the EDPB. In effect, the recent joint contribution by the EDPS-EDPB on the draft template relating to the description of consumer profiling techniques, recommends that when gatekeepers believe that the processing can rely on an alternative lawful legal bases, they should justify the reason(s) for relying on Articles 6(1)(c), (d) or (e) GDPR.[133]Therefore, it will not be an easy taskor gatekeepers

125 Recital 46 GDPR.
126 Information Commissioner's Office (2023) "Lawful basis for processing", p. 23.
127 *Supra*, Case C-252/21. Paras. 29 and 137.
128 Recital 45 GDPR.
129 Supra, Case C-252/21. Para. 133.
130 *Ibid*. Para. 134.
131 Supra, EDPB (2023) "Data protection guide for small business", Section 'Process personal data lawfully: public interest.' Available at https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en#toc-6
132 Supra, Information Commissioner's Office (2023), p. 26.
133 EDPB-EDPS Comments on the draft template relating to the audited description of consumer profiling techniques pursuant to Article 15 of the Digital Markets Act ('DMA') Adopted on 20 September 2023. Available at: https://edpb.europa.eu/system/files/2023-09/edps-edpb_comments_on_article_15_dma_template_report_for_plen_formatted.pdf (last access 9.11.2023).

to rely on these legal bases. The collection of the user's consent thus remains the main reasonable justification that gatekeepers could rely upon to continue its data combination activities under DMA.

4.2. Further Justifications in the DMA

Although it is not part of the objectives under discussion in this paper, a further interesting question connected to gatekeepers' obligations under the DMA, is whether and to what extent the gatekeeper could rely on 'additional' justifications, in comparison to those provided under Art. 5(2), to combine personal data without the user's consent. The gatekeeper could argue that data combination and cross-use may generate efficiency gains for the end user, in terms of improved product quality. Alternatively, the gatekeeper could argue that the data combination/cross-use may be necessary to prevent/detect online crimes, such as frauds.[134] While the EU Court of Justice recognized in *Post-Danmark I* that a dominant firm may rebut, at least in theory, the finding of abuse if it puts forward evidence showing that the alleged abusive behaviour is efficient and it benefits final consumers,[135] no such justification exists under the DMA. According to the Preamble, the DMA obligations are applicable "independently the actual, potential or presumed effects of the conduct of a given gatekeeper covered by this Regulation on competition on a given market."[136] In other words, unlike competition law, the gatekeeper cannot put forward an efficient defence to justify the lack of compliance with the DMA obligations.[137]

The space for objective justifications under the DMA is also rather limited: the gatekeeper could ask the EU Commission "to suspend" the application of a DMA obligation due to "exceptional circumstances beyond the gatekeeper control" in case such "exceptional circumstances" would "endanger (…) the viability of the gatekeeper activities in the Union."[138] According to the DMA Preamble, an exceptional circumstance would take place if an "unforeseen external shock" eliminated "a significant part of the end users' demand for the relevant core platform service."[139] An exceptional circumstance that could fulfil such high burden of proof is rather difficult to imagine. It is worth to point out that the exceptional circumstance should affect the end users 'demand', rather than the 'supply' of the core platform service. Consequently, exceptional events (e.g., natural catastrophe, pandemic, or a war in a region of the world) that would substantially affect the ability of an online intermediation service to sell products on its marketplace due to disruptions in the international supply chain would not qualify for a suspension of the DMA obligations; such exceptional events would affect the supply, rather than the demand of the core platform service. In addition, the suspension should be granted by the EU Commission on a temporary basis; the EU Commission should review on a "regularly basis" whether the exceptional circumstances are still in place, and thus whether and to what extent the suspension could be further either renewed, or terminated, or refined in relation to the different DMA obligations.[140]

Alternatively, the EU Commission could adopt a Decision, exempting a gatekeeper from applying specific DMA obligations due to reasons of 'public health' and 'public security'.[141] The DMA Preamble stresses the limited scope of these derogations. In particular, the EU Commission could adopt an exemption Decision only in "exceptional circumstances", in cases of public health and public security reasons "laid down in Union law."[142] The reference to EU law is rather important: it implies that the gatekeeper cannot ask for an exemption from a DMA obligation due to reasons of public health and security declared by an individual EU Member State; only a binding act adopted by the EU

134 Centre for Information Policy Leadership (CIPL) Discussion Paper, "Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences." Published in April 2023. P. 12. The paper is available at: https://www.informationpolicycentre.com/ (last access 18.5.2023).
135 Case C-209/10, *Post Danmark A/S v. Konkurrencerådet* (2012) ECLI:EU:C:2012:172. Para. 41-42.
136 *Supra,* Para. 11 DMA Preamble.
137 *Supra*, Moreno and Petit.
138 *Supra,* Art. 9(1) DMA.
139 *Supra,* Para. 66 DMA Preamble.
140 *Supra,* Para. 66 DMA Preamble.
141 *Supra,* Art. 10(1) DMA.
142 *Supra,* Para. 67 DMA Preamble.

institutions could meet this high burden of proof (e.g. EU Commission Decision; Council Regulation). In addition, the exemption would be temporary: the EU Commission would review the need for an exemption every year.[143] Similar to the suspension request, the exemption from the DMA obligations remains a truly exceptional circumstance. In relation to Art. 5(2) obligation, the EU Commission could grant an exemption to the prohibition of data combination/cross-use, for instance, in case a new pandemic hit Europe and some gatekeepers were asked to profile their users, to support the national health authorities to detect early on the latest pandemic developments. However, this exemption would not take place either because the gatekeeper spontaneously decided 'to help' the health care authorities, or because of a decision of a national government, but only because of a binding act adopted by the EU institutions.

In a nutshell, although the gatekeeper could argue that data combination, without the user's consent, is justified by the need to improve the service quality, as well as by security considerations, mostly related to the need to prevent online crimes, it is quite unlikely that the EU Commission would accept any of these justifications. The DMA, in fact, does not provide for efficiency defences. Secondly, the burden of proof faced by the gatekeeper to ask for an exemption/suspension from the DMA obligation is particularly high. The collection of the user's consent thus remains the main possibility for the gatekeeper to continue its data combination/cross-use activities within its own eco-system after the DMA entry into force.

5. Conclusions

The DMA obligations often derive from remedies previously adopted by competition authorities and by the EU Commission in the contest of previous antitrust investigations.[144] This is also the case for Art. 5(2) DMA, inspired by the 'data silos' remedy imposed by the *Bundeskartellamt* in its 2019 decision in the *German Facebook* case.[145] However, it is worth stressing that Meta will not be the only addressee of Art. 5(2) obligation; the latter provision will affect most of the designated gatekeepers. Data combination, in fact, is a common practice among the gatekeepers: it is a practice implemented by platforms that follow a target advertising business model (e.g., Meta, Tik Tok, Google), but also by online marketplaces (e.g., Amazon) as well as by apps, video and music stores (e.g., Apple) in order to personalize the search results of the end user.[146] Therefore, Art. 5(2) obligation is likely to impact the business models followed by most of the gatekeepers. The recent Bundeskartellamt commitment decision in the *German Google* case well represents the relevance of the data combination requirement for most of the designated gatekeepers under the DMA.[147]

Every gatekeeper will have to decide how to proceed with the implementation of the Art. 5(2) obligation: on the one hand, some gatekeepers might decide to change their business model, stopping combining/cross-using personal data across their eco-system, by thus relying on alternative sources of revenues in comparison to target advertising. The Meta recent announcement to offer a subscription version of Facebook and Instagram without ads goes in this direction.[148] Other gatekeepers, on the other hand, will rely on the exceptions provided by Art. 5(2) to continue data combination. The choice will be influenced by several factors; in particular, every gatekeeper will have to compare the economic relevance of data combination and users' profiling for its business model against Art. 5(2) compliance costs. The latter will include the technical costs in devising an effective system to collect the users' consent to data combination. In addition, the gatekeeper opting for continuing data combination should also take in consideration the risks of being later sanctioned by the EU Commission, NCAs as well as national civil courts in the context of private enforcement

143 *Supra,* Para. 67 DMA Preamble.
144 Friso Bostoen (2023), "Understanding the Digital Markets Act." 68(2) *Antitrust Bulletin:* 263-306. Table 3.
145 *Bundeskartellamt* decision in the *German Facebook* case, adopted on 6th February 2019, case number B.6/22-16. The decision is available, in the original German version, at: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568 (last access 18.5.2023).
146 *Supra,* CIPL discussion paper.
147 *Supra*, Bundeskartellamt decision in case B7-70/21.
148 https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/ (last access 9.11.2023).

actions, due to its inability to collect a 'valid' consent by end users authorizing data combination. Finally, the choice will be influenced by the expected success of a subscription model in the contest of markets where users have traditionally been used to receive services 'free of charge'.[149] Following a large empirical study, Akman has concluded that, although most of the consumers dislike the idea of target advertising carried out by large platforms, they would be nevertheless unwilling to pay a fee to get access to a social network without ads.[150] In view of the legal, technical and business uncertainty caused by such a radical change of the business modes, most of the gatekeepers might decide to offer two different types of services: an ads-free subscription based service, where data combination would not take place, as well as continuing offering a service based on target advertising, where data combination and cross-use would continue to take place subject to the user's consent in accordance with the privacy-setting requirements discussed in the previous pages. The recent Meta announcement to offer both a subscription-based and an ads-based version of Facebook goes in this direction, and it might soon be followed by other gatekeepers.

The paper has analysed the expected challenges faced by the gatekeepers that decide to continue data combination within their own eco-system after the DMA entry into force. In this regard, the user's consent is the main exception provided by Art. 5(2) DMA to the general prohibition of data combination and cross-use provided by this provision. In particular, the users' consent should comply with the general criteria for a valid consent indicated by Art. 7 GDPR.

In the paper, we have argued in favour of a 'privacy-setting' solution, introduced by the gatekeeper within its platform service: at the moment of the first log in, the user would face on his/her screen a cookie wall, asking her/him to opt-in to specific types of data combination activities by the gatekeeper. The gatekeeper would have the burden of explaining to the user, in a non-technical manner, the consequences of the opt-in choice, in terms of more personalised service and target advertising. Secondly, the user choice should be 'as granular as possible' – i.e., every data combination activity carried out by the gatekeeper among different core platform services should be subject to a specific opt-in request. After the first long in, the selected privacy setting would remain in force, but the user could always modify its preferences in terms of data combination.

Cookie walls have generally been considered not compatible with the GDPR requirement in terms of free consent. However, the initial ban on cookie walls followed by some data protection authorities has gradually changed, and a more flexible approach has been applied by some data protection authorities. In the online world, the emphasis on individual/repeated consent request for every data processing has generated the so-called 'consent fatigue'. In the paper, we have argued that the DMA anti-circumvention provision addresses the consent fatigue issue: in our view, if the gatekeeper had to ask for the user's consent every time before engaging in a data combination activity, this would represent a breach of Art. 13(6) DMA. Therefore, while respecting the general criteria indicated by Art. 7 GDPR, the users' consent under Art. 5(2) DMA should be 'adjusted' to the Digital Markets Act peculiarity. In our view, since the DMA and GDPR have the same status within the hierarchy of EU legal norms, and the DMA provides for a more specific legal framework in comparison to the GDPR, the DMA should be considered as a *lex specialis*, taking precedence over the GDPR in case of conflict.

The paper has also analysed whether and to what extent the gatekeeper could rely on the other exceptions provided by Art. 5(2), to carry out data combination activities without the user's consent. Art. 5(2) DMA, in fact, allows the gatekeeper to combine and cross-use data when the latter is necessary either to comply with a 'legal obligation' to which the gatekeeper is subject to, or to protect the 'vital interests' of the user, or to carry out a task in the 'public interest' or 'official authority' vested in the gatekeeper. These three legal bases for data processing provided by Art. 6 GDPR have recently been 'restrictively' interpreted by the CJEU in the *German Facebook* case. Such restrictive

149 Cristophe Carugati, 'The Pay-or-Consent Challenge for Platform Regulators.' Bruegel blog post published on 6.11.2023. The post is available at: https://www.bruegel.org/analysis/pay-or-consent-challenge-platform-regulators#footnote7_ygtz7tu (last access 9.11.2023).

150 Pinar Akman (2022) 'A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets' 16(2) *Virginia Law and Business Review:* 217.

interpretation should also be followed under Art. 5(2), since these legal bases represent exceptions to the general prohibition to data combination activities provided by this provision. For instance, the gatekeeper could engage in data combination activities, without the user's consent, to identify fraud and different types of online crimes only if so, requested by a public authority, such as the police or a public prosecutor. Such an interpretation is also supported by the other DMA provisions, which grant limited possibilities to the gatekeeper to ask the EU Commission to obtain a suspension/exemption from the DMA obligations.

Art. 5(2) falls under the list of DMA obligations that are self-executing. The EU Commission is thus not expected to clarify via the Decision to the designated gatekeeper how the latter should comply with this provision. As argued in the previous pages, however, compliance with Art. 5(2) DMA is far from being straightforward and clear; the data combination provisions should have been included under Art. 6 obligations (i.e., obligations that may be "further specified" by the EU Commission). It will be up to every gatekeeper to devise a compliance mechanism with the data combination prohibition, and eventually to design an effective system to collect the user's consent. The recent decisions adopted by the Bundeskartellamt in the contest of the *Facebook* and *Google* cases represent important precedents that could provide guidance to gatekeepers on how to comply with Art. 5(2) obligation.

Authors

Marco Botta

Robert Schuman Centre **/** European University Institute

marco.botta@eui.eu

Danielle Borges

Robert Schuman Centre / European University Institute

Danielle.Borges@eui