


ARTICLE

## The DMA's Consent Moment and its Relationship with the GDPR

Alessia S. D'Amico \*

International and European Law, Utrecht University, Utrecht, Netherlands  
Email: [a.s.damico@uu.nl](mailto:a.s.damico@uu.nl)

### Abstract

The Digital Markets Act (DMA) is designed to ensure fair and contestable digital markets. With one of the key sources of market power of big tech being data, it is not surprising that it is the subject matter of a number of DMA provisions. Article 5(2) prohibits gatekeepers from engaging in forms of accumulation and cross-use of personal data, unless they receive users' consent, defined by reference to the General Data Protection Regulation (GDPR).

Consent as defined by the GDPR suffers from a number of shortcomings, among other things, relating to whether consent can be truly freely given. The DMA tries to address some of the shortcomings by formulating a version of consent that seemingly goes beyond the GDPR. While a new version of consent may ensure greater effectiveness, it raises questions concerning the interaction and compatibility with the GDPR.

To shed light on this issue, the paper discusses the role and meaning of consent in the DMA vis-à-vis the GDPR and explores how to interpret consent under both the DMA and GDPR in a manner that is consistent with each other and that accounts for the characteristics of digital markets.

**Keywords:** consent; DMA; GDPR

### 1. Introduction

The Digital Markets Act (DMA)<sup>1</sup> is considered one of the centrepieces of the European digital strategy and aims to ensure the contestability and fairness of digital markets. This is done through rules which “address the risk of harmful effects of practices by gatekeepers, to the benefit of the business environment in the services concerned, of users and ultimately of society as a whole.”<sup>2</sup> Given data's central role in digital markets, it is not surprising that the DMA contains provisions controlling gatekeepers' conduct involving personal data, including data accumulation and data cross-use prohibitions.<sup>3</sup>

While the obligations under the DMA are aimed at increasing market contestability, to the extent that they concern the processing of personal data, they interrelate with the

---

\*Assistant Professor, Utrecht University, Netherlands.

<sup>1</sup> 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) 2019/137 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1.

<sup>2</sup> DMA, recital 31.

<sup>3</sup> DMA, Art 5.

General Data Protection Regulation (GDPR).<sup>4</sup> The DMA prohibits gatekeepers from engaging in specific forms of data accumulation and data cross-use, *unless* they receive users' consent. Consent under the DMA is defined by reference to the GDPR,<sup>5</sup> and, just as under the GDPR, requires users to be presented with a specific choice<sup>6</sup> and to be able to freely choose to opt-in to the data processing.<sup>7</sup>

However, consent as defined by the GDPR is not without its challenges, among other things, due to the proliferation of data processing online resulting in consent fatigue,<sup>8</sup> and the power imbalance between individuals and big tech.<sup>9</sup> Since the GDPR entered into force, the problem with placing the responsibility on individuals through the concept of consent has been criticised repeatedly.<sup>10</sup> One shortcoming, in particular, arises when individuals do not have a choice in concentrated markets. In this respect the power disparity between platforms and individuals may preclude the granting of GDPR-compliant consent, by hindering that consent is given freely.<sup>11</sup> By relying on consent, the DMA might suffer from the same shortcomings as the GDPR. Thus, it is questionable whether the functioning of the market can be improved by relying on individuals' choices in regard to data processing, instead of limiting the behaviour of gatekeepers directly.<sup>12</sup>

The provisions laying down the requirements for consent under the DMA reveal that the legislators were very well aware of the shortcomings surrounding consent. As a matter of fact, the rapporteur proposed to remove the option of consent, arguing that informed consent is "virtually unachievable" and instead opt for an outright prohibition.<sup>13</sup> Nonetheless, it was ultimately decided to include consent and instead tackle the shortcomings of the GDPR with more stringent consent requirements. Given that the DMA and GDPR both apply to gatekeepers when they are processing personal data, it is crucial for the DMA to be consistent with the GDPR and aim towards achieving complementary goals, rather than creating frictions by adopting clashing approaches.<sup>14</sup> Against this backdrop, the paper discusses the role and meaning of consent in the DMA vis-à-vis the

<sup>4</sup> 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) [2016] OJ L 119/1.

<sup>5</sup> GDPR, Art 7.

<sup>6</sup> DMA, Art 5(2).

<sup>7</sup> DMA, recital 36.

<sup>8</sup> EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020, paras 87–88.

<sup>9</sup> Alessia S. D'Amico, "Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given?" (2023) 8(2) European Papers – A Journal on Law and Integration, available at <https://doi.org/10.15166/2499-8249/678>.

<sup>10</sup> Bart W. Schermer, Bart Custers and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 Ethics and Information Technology 12; Daniela Messina, "Online Platforms, Profiling, and Artificial Intelligence: New Challenges for the GDPR and, in Particular, for the Informed and Unambiguous Data Subject's Consent" 16; Damian Clifford, Inge Graef and Peggy Valcke, "Pre-Formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections" (2019) 20 German Law Journal 679; Daniel Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law" (22 January 2023). Available at SSRN: <https://ssrn.com/abstract=4333743>.

<sup>11</sup> Damien Geradin, Konstantina Bania and Theano Karanikioti, "The interplay between the Digital Markets Act and the General Data Protection Regulation," p 9.

<sup>12</sup> Inge Graef, "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/>.

<sup>13</sup> European Parliament, Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on Contestable and fair markets in the digital sector (Digital Markets Act) 2020/0374(COD) (2.10.2021), p 4.

<sup>14</sup> EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, 10 February 2021, para 12.

GDPR and explores how to interpret consent under the DMA and GDPR in a manner that is consistent with each other and that accounts for the characteristics of digital markets.

## II. Consent under Article 5(2) DMA

The idea that underlies Article 5(2) DMA is that restricting gatekeepers' data accumulation will help create a level playing field between gatekeepers and other market players. Among other things, this is due to the fact that the gatekeepers' combination of personal data for the purpose of online advertising services may give them a competitive advantage and raise entry barriers.<sup>15</sup> Article 5(2) DMA lays down the following rule:

The gatekeeper shall not do any of the following:

- (1) *process*, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper;
- (2) *combine* personal data from the relevant core platform service with personal data ... from any other services provided by the gatekeeper or with personal data from third-party services;
- (3) *cross-use* personal data from the relevant core platform service in other services provided separately by the gatekeeper ... and
- (4) *sign in* end users to other services of the gatekeeper in order to combine personal data,

unless the end user has been presented with the specific choice and has given consent within the meaning of Article 4, point (11), and Article 7 of Regulation (EU) 2016/679 ...<sup>16</sup>

Accordingly, Article 5(2) does not contain an outright prohibition of data processing, but rather a restriction of it; gatekeepers shall not process data in set ways, *unless* they receive consent within the meaning of the GDPR.<sup>17</sup> Here an overlap between the DMA and the GDPR is created, since the GDPR is already applicable to the forms of data processing contained in Article 5(2).<sup>18</sup>

A closer look at the text of the DMA reveals that, although it relies on the GDPR, it appears to go beyond it in limiting data processing in two ways: (1) mandating that gatekeepers receive users' consent for determinate forms of processing (precluding other potential legal bases) and (2) specifying additional requirements for users' consent.

### 1. Consent as the only legal basis for data processing

Article 5(2) of the DMA states that it is without prejudice to the possibility for the gatekeeper to rely on "legal obligation," "vital interests" and "public interest" as legal bases for processing under the GDPR. It does not make an exception for the legal bases of

<sup>15</sup> DMA, recital 36.

<sup>16</sup> DMA, Art 5(2) (emphasis added).

<sup>17</sup> GDPR, Art 4(11) and 7.

<sup>18</sup> Under the GDPR, all processing of personal data, including the forms of processing covered by Article 5(2) DMA, must have a legal basis. The six legal bases under the GDPR are: consent, contract performance, legal obligation, vital interests, public interest and legitimate interests (GDPR, Art 6).

“contract performance”<sup>19</sup> and “legitimate interests.”<sup>20</sup> Recital 36 DMA more explicitly mentions that it is not possible for gatekeepers to rely on contract performance and legitimate interests for the forms of data processing contained in Article 5(2).<sup>21</sup> Although gatekeepers may rely on legal obligations, vital interests and public interest, these legal bases are, generally speaking, not suitable for the forms of processing covered by Article 5(2) DMA.<sup>22</sup> Thus, while under the GDPR data controllers can choose which legal basis is the most appropriate for determinate forms of data processing, under the DMA gatekeepers effectively have no choice but to use consent.

The impact of Article 5(2) DMA on gatekeepers’ data processing depends, partially, on the extent to which the GDPR legal bases beyond consent (legitimate interests and contract performance) would be available in practice for the types of processing listed in Article 5(2). If, also under the GDPR, these types of processing could only be made lawful through consent, Article 5(2) does not further limit gatekeepers in terms of the legal bases available. Since the processing addressed in Article 5(2) DMA is intended to cover “processing for the purpose of providing online advertising services,”<sup>23</sup> this section looks at the way the GDPR has been applied to those forms of processing.

In the opinion on the DMA proposal, the European Data Protection Supervisor (EDPS) pointed out that under the GDPR all data processors, irrespective of their position on the market, must obtain consent from end-users to combine personal data for the purposes of profiling and tracking.<sup>24</sup> A similar stance was also taken in earlier guidelines by the European Data Protection Board (EDPB), from which it can be derived that both legitimate interests and contract performance have a very little, if any, role to play in legitimising the forms of data processing contained in Article 5(2) DMA.<sup>25</sup> Several GDPR-related rulings against Meta in Germany,<sup>26</sup> Ireland,<sup>27</sup> and Norway,<sup>28</sup> and by the EDPB<sup>29</sup>

<sup>19</sup> GDPR, Art 6(1)(b), “processing is necessary for 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.”

<sup>20</sup> GDPR, Art 6(1)(f), “processing is necessary for the 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 ... ”

<sup>21</sup> DMA, recital 36.

<sup>22</sup> GDPR, Art 6(1)(c), (d) and (e). See CIPL, ‘Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences’, Discussion paper May 2023, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_dma\\_limiting\\_legal\\_basis\\_may2023.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf).

<sup>23</sup> DMA, recital 36.

<sup>24</sup> EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, 10 February 2021, para. 24.

<sup>25</sup> This was also confirmed by the EDPB’s decisions on Meta (see also below). In December 2022 the EDPB adopted three Arts 65 dispute resolution binding decisions regarding Facebook, Instagram and WhatsApp, in which it found that processing of personal data for the performance of a contract is not a suitable legal basis for behavioural advertising (Binding Decision 4/2022; Adopted on 5 December 2022). In the October 2023 the EDPB went further, imposing a ban on Meta for the processing of personal data for behavioural advertising purposes on the basis of contract and legitimate interests (Urgent Binding Decision 01/2023; 27 October 2023).

<sup>26</sup> Bundeskartellamt, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (B6-22/16 – 6 February 2019); case summary available at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsufsicht/2019/B6-22-16.html>.

<sup>27</sup> Irish DPA Final Decision against Meta Platforms Ireland Limited, 31 December 2022. Facebook service – DPC Inquiry Reference: IN-18-5-5, available at <https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20DECISION%20%28ADOPTED%29%2031-12-22%20-%20IN-18-5-5%20%28Redacted%29.pdf>;

Instagram service – DPC Inquiry Reference: IN-18-5-7, available at <https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20Decision%20%28ADOPTED%29%20-%20IN-18-5-7%20-%2031-12-22%20%28Redacted%29.pdf>.

<sup>28</sup> Datatilsynet, press release of 31 October 2023, <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/datatilsynets-vedtak-mot-meta-utvides-til-eueos-og-gjores-permanent/>.

<sup>29</sup> EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by Meta, [https://www.edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta\\_en](https://www.edpb.europa.eu/news/news/2023/edpb-urgent-binding-decision-processing-personal-data-behavioural-advertising-meta_en).

and the CJEU<sup>30</sup> have confirmed that consent is the only lawful legal basis for the purposes of behavioural advertising. The most recent decision in this regard is the one taken by the EDPB in October 2023, in which it unequivocally found that Meta could not rely on contract and legitimate interests for behavioural advertising purposes.<sup>31</sup> I will now have a closer look at how contract performance and legitimate interests have been applied in the context of behavioural advertisement.

### *a. Contract performance*

In terms of contract performance under Article 6(1)(b) GDPR, the Article 29 working party stressed that this legal basis must be interpreted strictly and only applies if the processing is genuinely necessary for the performance of a contract, as opposed to be unilaterally imposed by the data controller.<sup>32</sup> In order to determine this, one needs to look at the rationale of a contract and against this assess whether the processing is necessary for its performance.<sup>33</sup> The EDPB argued that personalisation may constitute an intrinsic and expected element of an online service, depending on the nature of the service, the expectations of users and whether it could also be provided without personalisation.<sup>34</sup> When personalisation is merely aimed at increasing user engagement, for instance, it cannot be considered an integral part of a service, and a different legal basis needs to be relied on.<sup>35</sup> Similarly, in the guidelines on targeting of social media users, the EDPB clarified that “in respect to the social media providers Article 6(1)b GDPR cannot provide a lawful basis for online advertising simply because such advertising indirectly funds the provision of their service.”<sup>36</sup>

In the Irish DPA's decision against Meta in respect of the Instagram service,<sup>37</sup> the Commissioner argued that “the mere inclusion of a term in a contract does not necessarily mean that it is necessary for the performance of that contract; rather, a functional assessment of the specific contract should take place.”<sup>38</sup> She found that Meta Ireland was not entitled to rely on Article 6(1)(b) GDPR to process personal data for the purpose of behavioural advertising in the context of the Instagram Terms of Use. In the decision she refers to the guidelines of the EDPB, which state that processing cannot be rendered lawful by Article 6(1)(b) GDPR “simply because processing is necessary for the controller's wider business model”<sup>39</sup> and that “normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads.”<sup>40</sup> Similarly, in the *Meta* judgment,

<sup>30</sup> Case C-252/21 *Meta Platforms and Others*, ECLI:EU:C:2023:537, 4 July 2023.

<sup>31</sup> EDPB, Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR), Adopted on 27 October 2023, available at [https://edpb.europa.eu/system/files/2023-12/edpb\\_urgentbindingdecision\\_202301\\_no\\_metaplatformsireland\\_en\\_0.pdf](https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf).

<sup>32</sup> Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), p 16.

<sup>33</sup> *Ibid.*

<sup>34</sup> EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Version 2.0 (8 October 2019) available at [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf), para. 56.

<sup>35</sup> *Ibid.*, para. 57.

<sup>36</sup> EDPB, “Guidelines 8/2020 on targeting of social media users,” Version 2.0 (13 April 2021), para. 49, available at [https://edpb.europa.eu/system/files/2021-04/edpb\\_guidelines\\_082020\\_on\\_the\\_targeting\\_of\\_social\\_media\\_users\\_en.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf).

<sup>37</sup> Irish DPA Final Decision against Meta Platforms Ireland Limited, 31st December 2022 (Instagram service - DPC Inquiry Reference: IN-18-5-7), available at <https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20Decision%20%28ADOPTED%29%20-%20IN-18-5-7%20-%2031-12-22%20%28Redacted%29.pdf>.

<sup>38</sup> *Ibid.*, para 89.

<sup>39</sup> Guidelines 02/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0 (adopted 8 October 2019), para 36.

<sup>40</sup> *Ibid.*, para 52.

the ECJ stated that when it comes to personalised content, it “does not appear to be necessary in order to offer that user the services of the online social network.”<sup>41</sup>

#### *b. Legitimate interests*

Article 6(1)(f) requires a balancing between the legitimate interests of the data controllers and the interests and rights of the data subjects, taking into account data subjects’ reasonable expectations.<sup>42</sup> In *Fashion ID*, the ECJ reiterated that for this legal basis to be relied on, three conditions must be satisfied:

first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence.<sup>43</sup>

The EDPB points out that the “necessity” requirement ensures that the “legitimate interests” legal basis is not interpreted too broadly; it calls for an assessment of whether “less invasive means are available to serve the same end.”<sup>44</sup> In the same guidelines, the EDPB explicitly states that it would be difficult to justifying intrusive profiling and tracking practices for advertising purposes under a legitimate interests legal basis.<sup>45</sup>

In its abuse of dominance case against Facebook, the German competition authority looked at Facebook’s data combination practices and found that its interest in processing data did not outweigh the legitimate interests of users. In its decision, the authority took into account the type of data processed, the type of processing, the consequences for the users and their reasonable expectations. Interestingly,<sup>46</sup> it also took into consideration that Facebook was a dominant company, giving it the power to impose far-reaching data processing conditions unconstrained from users.<sup>47</sup> In the preliminary ruling on this case, the ECJ found that users cannot reasonably expect their personal data to be used for personalised advertising.<sup>48</sup> Accordingly, the interests and fundamental rights of users override the interest of Meta in relation to personalised advertising used to finance its activity and, thus, the processing cannot be based on a legitimate interest legal basis.

Although only a case-by-case assessment can determine which legal basis is valid for specific types of processing under the GDPR, it appears that in most cases consent will be the only adequate legal basis for the types of data processing listed in Article 5(2) DMA. Thus, by excluding contract performance and legitimate interests, the DMA does not substantially depart from the pre-existing GDPR obligation to have a legal basis under Article 6 GDPR. Even though this alignment means that the added value of the DMA in this regard is limited, by explicitly restricting the legal bases to consent, the DMA creates certainty and pre-empts discussions around when other legal bases may be relied on.<sup>49</sup>

<sup>41</sup> Case C-252/21 *Meta Platforms and Others*, ECLI:EU:C:2023:537, 4 July 2023, para 102.

<sup>42</sup> GDPR, recital 47.

<sup>43</sup> Case C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, para 95.

<sup>44</sup> EDPB, ‘Guidelines 8/2020 on targeting of social media users’, Version 2.0 (13 April 2021), para 52.

<sup>45</sup> *Ibid*, para. 56.

<sup>46</sup> It is exactly this case that inspired Article 5(2) DMA and it illustrates the connection between market power and data protection.

<sup>47</sup> Bundeskartellamt, Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (B6-22/16 - 6 February 2019); case summary available at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html>, pp. 10–11.

<sup>48</sup> Case C-252/21 *Meta Platforms and Others*, ECLI:EU:C:2023:537, 4 July 2023, para 117.

<sup>49</sup> As in the EDPB decisions against Meta.

Where the DMA might depart from the GDPR, is in relation to the *requirements* of valid consent. This is what the next section will explore.

## 2. Requirements of valid consent: DMA vs GDPR

Formally, the DMA does not introduce a distinct notion of consent, but it relies on the version of consent contained in the GDPR.<sup>50</sup> Both regulations use the keywords “freely given,” “specific,” “informed,” “unambiguous,” refer to an affirmative action,<sup>51</sup> and stress the importance of an easy withdrawal of consent.<sup>52</sup> Supporting the understanding of consent under the DMA as GDPR consent, Geradin et al. argue that “this is not surprising given that consent is a well-established concept under EU data protection law. Therefore, all the requirements and standards the GDPR establishes in relation to requesting user consent remain applicable in the context of consent being required under the DMA.”<sup>53</sup>

Nonetheless, a closer look at the recitals of the DMA reveals that the intent may be for consent under the DMA to go beyond the GDPR. Table 1 below juxtaposes provisions from the DMA and GDPR relating to requirements for valid consent that are comparable but not fully equivalent.

Table 1 shows that the DMA introduces some additions compared to the GDPR, when it comes to the rules concerning the requirements for valid consent, in particular relating to the “informed,” “unambiguous” and “freely given” aspects of consent.<sup>54</sup>

### a. Informed and unambiguous

The DMA explicitly mentions that gatekeepers should not design their “online interfaces in a way that deceives, manipulates” and that they should “proactively present a user-friendly solution.” These formulations are more explicit as to the manner in which consent shall be requested in a digital environment, hinting to the problematics of dark patterns. As such, they appear to go further than the corresponding provisions in the GDPR, which more generally state that consent needs to be requested in an “intelligible and easily accessible form, using clear and plain language.” Furthermore, the DMA explicitly mentions that consent cannot be requested more than once a year; this temporal restriction is lacking in the GDPR.

While the DMA provisions are more explicit than the corresponding GDPR provisions, it is debatable to what extent these depart from the way the related GDPR provisions have been applied in practice. For instance, the DMA refers to “online interfaces” and “user-

<sup>50</sup> GDPR, Art. 4(11) and 7.

<sup>51</sup> DMA: “the end user has been presented with the specific choice and has given consent within the meaning of [the GDPR]” (Art 5(2)); “consent should be given by a clear affirmative action or statement establishing a freely given, specific, informed and unambiguous indication of agreement by the end user”(recital 37); “gatekeepers should enable end users to freely choose to opt-in” (recital 36).

GDPR: “‘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” (Art 4(11)); “Silence, pre-ticked boxes or inactivity should not therefore constitute consent” (recital 32).

<sup>52</sup> DMA: “Not giving consent should not be more difficult than giving consent” (recital 37). GDPR: “It shall be as easy to withdraw as to give consent” (Art 7(3)).

<sup>53</sup> Damien Geradin, Konstantina Bania and Theano Karanikioti, “The interplay between the Digital Markets Act and the General Data Protection Regulation,” p 8.

<sup>54</sup> For more on the sources of these requirements see Cristiana Santos, Nataliia Bielova and Célestin Matte, “Are cookie banners indeed compliant with the law?” (2020) Technology and Regulation, 91–135, available at <https://doi.org/10.26116/techreg.2020.009>. See also EDPB Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, 4 May 2020, available at [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf).

Table I. Consent in the DMA vs GDPR.

DMA	GDPR
<i>Informed &amp; Unambiguous</i>	
“Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent” (recital 37).	“[A] declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms” (recital 42).
“When the gatekeeper requests consent, it should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner” (recital 37).	“[T]he request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language” (Article 7(2)) [also Articles 12(1) and 13(2)(c) GDPR].
“Gatekeepers should not be allowed to prompt end users more than once a year to give consent for the same processing purpose in respect of which they initially did not give consent or withdrew their consent” (recital 37).	“[T]he request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided” (recital 32).
<i>Freely given (unconditional)</i>	
Gatekeepers should not make “the use of the core platform service or certain functionalities thereof conditional upon the end user’s consent” (recital 36).	“When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract ... is conditional on consent to the processing of personal data that is not necessary for the performance of that contract” (Article 7(4)).
“[G]atekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative ...” (recital 36) “The less personalised alternative should not be different or of degraded quality ...” (recital 37).	

friendly” solutions and in the GDPR consent guidelines the EDPB state: “To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.”<sup>55</sup> The French DPA explains that methods chosen to make information accessible can vary and can include “pop-ins, tooltips, dedicated pages, QR code, audio messages, videos, display boards, paper documentation, information campaigns, etc”<sup>56</sup> and that “it is necessary to provide the most relevant information at the right time ... provide a first level of information and highlight the important characteristics of processing.”<sup>57</sup>

As to the temporal restriction, although there is no direct equivalent in the GDPR, undue pressure exerted by frequent requests for consent could also invalidate GDPR consent, if it is disruptive to the use of the service for which it is provided.<sup>58</sup> For example, the Italian DPA stated that consent for cookies cannot be repeated more than once every six months.<sup>59</sup>

<sup>55</sup> EDPB Guidelines 05/2020 on consent, para 71.

<sup>56</sup> CNIL – Data & Design by LINC, available at <https://design.cnil.fr/en/concepts/information/>.

<sup>57</sup> *Ibid.*

<sup>58</sup> GDPR, recital 32.

<sup>59</sup> Garante per la protezione dei dati personali, ‘Linee guida cookie e altri strumenti di tracciamento’ 10 june 2021 [9677876] <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english>.

### b. Freely given

In relation to the provisions relating to the freely given aspect of consent, both the DMA and the GDPR establish that access to the service cannot be made conditional on users' consent.<sup>60</sup> The key difference, however, lies in the emphasis in the DMA on the mandatory opt-out requirement linked to the obligation to offer a less personalised but equivalent alternative, which, in this form, is absent in the GDPR. The GDPR merely establishes that: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."<sup>61</sup> In regard to this provision, the EDPB's guidelines state that the legislator's emphasis on conditionality as a presumption of a lack of freely given consent indicates the importance of closely examining instances of conditionality. Despite the relevance of conditionality when determining if consent is freely given, the formulation "utmost account" in Article 7(4) comes short of creating a prohibition on conditionality and must be regarded as a presumption. In *Planet49*,<sup>62</sup> for instance, an online gaming company held an online promotional lottery that required users to reveal personal information in exchange for participation. The Advocate General<sup>63</sup> saw no problem with the "selling" of personal data, arguing that "it is the providing of personal data which constitutes the main obligation of the user in order to participate in the lottery. In such a situation it appears to me that the processing of this personal data is necessary for the participation in the lottery".<sup>64</sup>

This debate around conditionality and freely given consent under the GDPR has also played a significant role *Meta*,<sup>65</sup> in which the ECJ answered key questions regarding the application of the GDPR vis-à-vis dominant platforms. The Court held that, in the case of dominant companies:

those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.<sup>66</sup>

This reads very much like the provision in the DMA that requires gatekeepers to provide an equivalent service without data processing, in order for consent to be valid.<sup>67</sup> In the

<sup>60</sup> The GDPR does not contain an outright prohibition, but states that 'utmost account' will be given to this (Art 7(4)).

<sup>61</sup> GDPR, Art 7(4).

<sup>62</sup> Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, ECLI:EU:C:2019:801.

<sup>63</sup> Case C-673/17, Opinion of Advocate General Szpunar delivered on 21 March 2019 in *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:246.

<sup>64</sup> Case C-673/17, Opinion of Advocate General Szpunar, para. 99. The AG refers to Buchner, J., Kühling, B., in J. Buchner, B. Kühling (eds), *Datenschutz-Grundverordnung/BDSD, Kommentar*, 2nd ed. 2018, C.H. Beck, Munich, Artikel 7 DS-GVO, point 48. The Court did not raise the question around Article 7(4) GDPR, noting that the referring court had not referred to it the question whether the conduct was compatible with the requirement that consent be 'freely given', Case C-673/17, *Planet49*, ECLI:EU:C:2019:801, para 64.

<sup>65</sup> Case C-252/21, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2023:537.

<sup>66</sup> C-252/21, para 150.

<sup>67</sup> In its consent guidelines the EDPB had also suggested that to enable users to choose freely, a controller could offer users a "choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand" (EDPB Guidelines 5/2020 of 4 May 2020 on consent under Regulation (EU) 2016/679, para 37).

legislative proposal, the Commission indicated that the DMA complements the GDPR, specifying that “mandatory opt-out for data combination across core platform services supplements the existing level of protection under the GDPR”<sup>68</sup> and in the impact assessment report it states that “mandatory opt-out for data combination across core platform services goes beyond GDPR protections.”<sup>69</sup> When it comes to provisions relating to freely given consent, it does appear that while the safeguards included in the DMA reflect the GDPR, they might go further in setting out explicit requirements that the gatekeepers must meet to obtain valid consent under the GDPR.<sup>70</sup> In particular, the DMA seems to close the GDPR’s gap in terms of conditionality of consent.

Although the DMA does not impose entirely novel requirements for valid consent compared to the GDPR, it does seem that, when it comes to freely given consent, it is more precise and rigorous in the way the requirements are intended to be applied. While the GDPR leaves some flexibility as to when conditionality is allowed, and to what degree, the DMA is more categorical in this regard. If the requirements are indeed applied more stringently under the DMA than under the GDPR, this could give rise to incoherence between the regulations. The way the DMA’s mandatory opt-out and equivalent service requirements are applied in practice can have significant repercussions on the digital market. This is due to the fact that, in contrast to rules regarding the way in which consent is requested, the rules on conditionality have the potential to impact the very business model of online platforms. It is, thus, imperative to have clarity on the implications of the DMA on conditionality as understood previously under the GDPR. In the next section I will analyse in more detail the rules on conditionality and propose how the DMA and GDPR can be interpreted in a coherent way in this regard.

### III. A coherent and effective version of consent

The text of the DMA indicates that it shall apply “without prejudice” to the GDPR.<sup>71</sup> As explained by Bania, this formulation means that DMA obligations are applicable without detriment to any existing right enshrined in the GDPR.<sup>72</sup> However, the DMA fails to establish which legislation would prevail in the case of divergent interpretations. With both being EU regulations, the DMA and the GDPR have equal status within the hierarchy of EU legal norms. Nonetheless, the DMA regulates a more specific form of conduct than the GDPR, which, in contrast, is horizontally applicable to all forms of personal data processing. In light of the principle *lex specialis derogat generali*, in the case of conflict between the DMA and the GDPR, the former should prevail.<sup>73</sup> As the DMA and GDPR are applicable to the same digital platforms, however, introducing different requirements for valid consent would further increase the complexity of this multi-layered regulatory environment. It would potentially lead to a situation in which gatekeepers would have to obtain one form of consent for personal data processing that falls under Article 5(2) DMA and another one for all other types of personal data processing. The fact that the DMA explicitly relies on the definition of consent in the GDPR shows that the legislators’

<sup>68</sup> Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final (emphasis added).

<sup>69</sup> Commission Staff Working Document Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) SWD/2020/363 final (Brussels, 15.12.2020) (emphasis added).

<sup>70</sup> Damien Geradin, Konstantina Bania and Theano Karanikioti, ‘The interplay between the Digital Markets Act and the General Data Protection Regulation’, p 10.

<sup>71</sup> DMA, recital 12.

<sup>72</sup> Konstantina Bania ‘Fitting the Digital Markets Act in the Existing Legal framework: the Myth of the Without Prejudice Clause’ (2023) 19(1) European Competition Journal, p 117.

<sup>73</sup> *Ibid*, p 148.

intention was not to introduce a separate consent requirement, but to align DMA consent with GDPR consent. It is, thus, desirable to adopt a version of consent that is both coherent among the two regulations and that accounts for the characteristics of digital markets.

As identified above, it is particularly pressing to tackle the divergence between the two regulations when it comes to the extent to which users must be allowed to access a service without providing personal data. When enforcing the DMA, the Commission pursues a different objective than the one pursued by DPAs under the GDPR. A core objective of the DMA and of Article 5(2) is to promote market contestability. One concern in particular is that gatekeepers “feature an ability to connect many business users with many end users through their services, which, in turn, enables them to leverage their advantages, such as their access to large amounts of data, from one area of activity to another.”<sup>74</sup> Article 5(2) is enforced with this objective in mind. If, in concentrated markets, gatekeepers do not offer a genuine choice to users in terms of consenting to data processing, Article 5(2) will be utterly ineffective. The very nature of the markets in which the DMA applies calls for a rigorous approach to consent. In these markets, users do not have alternative services to switch to, so the only way to guarantee a choice, and to create a level-playing field with potential market entrants, is for users to be able to opt out of the processing and still use the gatekeepers’ service.

Consequently, the DMA envisages the possibility for a data controller to offer two options to users, one that involves the forms of data processing under Article 5(2) and an equivalent one that does not involve these forms of processing (and that may be offered for a fee instead).<sup>75</sup> Whether consent for the first option is freely given is said to depend on whether the second option, which does not involve consenting to the forms of data processing under Article 5(2), is a truly equivalent service.<sup>76</sup>

While the text of the DMA expressly mentions the equivalent service route, this requirement is more indirect in the GDPR. As discussed above, since the formulation ‘utmost account’ in the GDPR allows for (limited) flexibility, there may be situations where this conditionality does not automatically invalidate consent.<sup>77</sup> The economic value of personal data in the digital economy has led to the creation of business models in which digital content and services are offered in exchange for personal data. When regulating these transactions, the GDPR is not concerned with the market functioning, but the protection of individuals’ rights over data, including the right to consent to data processing.<sup>78</sup> Data protection is understood as a transparency tool, promoting individuals’ proactive right to *control* what happens with their data.<sup>79</sup> Control over data includes the right to share data, also in exchange for the access to content or services.<sup>80</sup> Thus, the flexibility surrounding the conditionality requirement contained in Article 7(4) is consistent with the objective of the GDPR. According to Kostić and Penagos, the legislative

<sup>74</sup> DMA, recital 3.

<sup>75</sup> Alexandre De Streel and Giorgio Monti, ‘Data-Related Obligations In the DMA’, Centre on Regulation in Europe (CERRE), *Implementing the DMA: Substantive and Procedural Principles*, (January 2024) available at [https://cerre.eu/wp-content/uploads/2024/01/CERRE.BOOK\\_DMA\\_17JAN.pdf](https://cerre.eu/wp-content/uploads/2024/01/CERRE.BOOK_DMA_17JAN.pdf), p. 71.

<sup>76</sup> DMA, recital 37: “The less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service.

<sup>77</sup> EDPB Guidelines 05/2020 on consent, paras 34–35.

<sup>78</sup> Article 8 of the Charter of Fundamental Rights, which the GDPR relies on, specifically mentions that personal data “must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”, Charter of Fundamental Rights of the European Union [2012] OJ C326/391, Art 8.

<sup>79</sup> GDPR, recital 7.

<sup>80</sup> “Privacy can essentially be described as a form of information management, where control is achieved through the expression of an individual’s preferences”. Henry Pearce, “Could the doctrine of moral rights be used as a basis for understanding the notion of control within data protection law?” (2018), p 137.

history of the provision “shows that the legislator consciously departed from an outright prohibition [of conditionality], and instead opted for a more nuanced approach.”<sup>81</sup>

Even if the exchange of data against digital content or services is not problematic in itself, the GDPR emphasises the need for consent to data processing to be “freely given,” for which a genuine choice must be provided. A lenient application of Article 7(4) is arguably justified in situations in which individuals can effectively choose whether to use a service that comes with data collection. When consumers have multiple options in a competitive market, it appears legitimate to leave the discretion to firms as to what kind of data to request in return for their services.<sup>82</sup> In these cases it can be assumed that consumers would only agree to the terms if they considered them fair in relation to what they are getting in return, making their consent freely given.<sup>83</sup>

On the contrary, in the case of controllers with significant market power, such as Meta, there is not a sufficient degree of competition in the market that would guarantee consumer choice. The Court in *Meta* explained that “the existence of such a dominant position may create a clear imbalance, within the meaning of recital 43 of the GDPR, between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the contract.”<sup>84</sup> One interpretation of the *Meta* judgment is that what is problematic is when *dominant* data controllers impose conditions that are not strictly necessary for the performance of a contract. This is due to the impact that market power has on the ability of individuals to choose, which is compromised when individuals do not have an adequate alternative on the market.

In order to protect individuals’ control over data it is, thus, justifiable to prohibit that gatekeepers make provision of their services conditional on consent to terms that go beyond what is necessary for the provision of their services. Instead, they should be ordered to give users a real choice (in terms of opting in or out) for consent to be valid.<sup>85</sup> Under both regulations, the GDPR and DMA, imbalance of power is a relevant factor when determining whether consent is valid.<sup>86</sup> If market power is taken into account in the GDPR as well, the concepts of consent converge. The GDPR squares with the DMA, if it is read in a way that consent given to gatekeepers can only be freely given, if data subjects have the chance to opt out from the processing that is not necessary for the provision of the service and still use the service.

Beyond establishing the existence of this convergence, it will need to be determined what the personalised and non-personalised version of a service must look like in order for consent to be valid. This is something that has not been subject to much debate yet, but it appears that two aspects will require scrutiny. Firstly, it will need to be determined what an equivalent, non-personalised, service must look like. The DMA clarifies that “the less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data . . . .”<sup>87</sup> Accordingly, the gatekeeper must be able to show that the decreased quality of the

<sup>81</sup> Bojana Kostić and Emmanuel Vargas Penagos, “The freely given consent and the ‘bundling’ provision under the GDPR Artikelen” (August 2017) Afl. 4, Computerrecht 2017/153, p. 220.

<sup>82</sup> As long as they obtain informed, specific, and unambiguous consent.

<sup>83</sup> This refers only to the freely given element of consent; there are other issues around consent, for instance whether it can ever be truly informed.

<sup>84</sup> Case C-252/21, *Meta Platforms and Others*, para 149.

<sup>85</sup> This differentiation applies to the determination of the lawfulness of processing (GDPR, Art. 6), more specifically, whether undertakings can use consent as a legal basis for processing. The other data protection principles (e.g. purpose limitation and data minimisation, GDPR, Art. 5) remain unaltered.

<sup>86</sup> See Case C-252/21, *Meta Platforms and Others*.

<sup>87</sup> DMA, recital 37.

non-personalised service vis-à-vis the personalised one is related to the fact that the feature in question can only be offered if the user consents to the collection of data otherwise forbidden by Article 5(2) DMA.

Secondly, the fee charged for the non-personalised service, if there is one, will need to be scrutinised. In the text of the DMA there is no indication as to how high a potential fee may be. However, it seems evident that it must be proportionate to the service offered, in order to constitute a realistic alternative to the personalised service. For instance, it is questionable, whether the fee that Meta started charging users for the non-personalised version of Facebook and Instagram of €9.99 or €12.99 per month (dependent upon where it is purchased) is appropriate.<sup>88</sup> The Commission and DPAs will certainly have to address these issues, when examining equivalent services in the context of freely given consent in the DMA and the GDPR in the future.

In 2023, the Commissioner for Justice and Consumers initiated a reflection on how to better empower consumers to make effective choices regarding tracking-based advertising models. The Commission proposed principles for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices. One of the principles is that in case of tracking-based advertising, it should not be sufficient for data controllers to offer a paid option, in order to rely on consent. A third option should be provided, which allows for a less intrusive form of advertising, such as contextual advertising. The reason submitted for this is that consumers are rarely willing to pay for online content and navigate numerous websites daily and that thus “asking consumers to pay does not appear a credible alternative to tracking their online behaviour for advertising purposes that would legally require to obtain consent.”<sup>89</sup> In its reply to the Commission’s initiative, the EDPB noted that whether offering a paid alternative ensures valid consent for tracking users for advertising purposes can only be assessed on a case-to-case basis. When determining this, a relevant factor is whether, in addition to the service which tracks users and the paid service, another more privacy friendly service is made available, for instance, one relying on contextual advertising.<sup>90</sup>

When speaking about freely given consent, it is apparent why merely offering a non-personalised paid option might not, in itself, make consent for the personalised version freely given. This is particularly the case when the paid version is costly and if one considers individuals’ inherent biases leading to the so-called “privacy paradox.”<sup>91</sup> However, under the DMA and GDPR the paid alternative route has now been put forward as an option when consent is collected for behavioural advertisement. While it is not yet entirely clear what this option has to look like, it is too early to dismiss it, and instead, it is desirable to better understand how it fits within the existing regulatory framework. This paper has tried to show that consent under the two regulations can, and should, be read in a consistent manner. The result is a post-DMA continued existence of only one form of consent, ie GDPR consent, which can be adapted to the characteristics of digital markets and the position of gatekeepers.

<sup>88</sup> Meta, ‘Facebook and Instagram to Offer Subscription for No Ads in Europe’ (30 October 2023) available at <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>.

<sup>89</sup> European Commission, ‘Draft Pledging Principles’, available at [https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge\\_en](https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en).

<sup>90</sup> EDPB, “EDPB reply to the Commission’s Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices” (19 December 2023) p 5, available at [https://edpb.europa.eu/system/files/2023-12/edpb\\_letter\\_out20230098\\_feedback\\_on\\_cookie\\_pledge\\_draft\\_principles\\_en.pdf](https://edpb.europa.eu/system/files/2023-12/edpb_letter_out20230098_feedback_on_cookie_pledge_draft_principles_en.pdf).

<sup>91</sup> Although individuals state that they would prefer to protect their personal information, they continuously contradict their stated preference by disclosing data; see Andrea Carignania and Vanessa Gemmo “New Media and Privacy the Privacy Paradox in the Digital World: I Will Not Disclose My Data. Actually, I Will ... It Depends” (2017) 27(1) *International Journal of Computer* 201–212.

#### IV. Conclusion

The DMA constitutes an important step towards ensuring fair and contestable digital markets. However, its consent-based approach under Article 5(2) has raised questions as to its effectiveness, as well as possible overlaps and conflicts with the GDPR. It appears that the relevant DMA provisions are more explicit with regard to requirements of valid consent, in particular the mandatory opt-out, and can be applied in a way that imposes obligations that go beyond the GDPR. To avoid inconsistencies and create synergies around the requirement of consent for data processing, this paper has put forward a reading of the GDPR and DMA that renders their consent requirements consistent with each other and suitable for the digital market. The analysis of the provisions relating to consent under the DMA and GDPR, in light of their regulatory objectives, revealed that it is possible to interpret the provisions in a compatible way.

If the Commission and DPAs agree on a common reading of consent and an understanding of what valid consent in case of market dominance, such as in the case of gatekeepers, must entail, not only would the Commission be able to apply consent as currently understood in the GDPR, but DPAs could also apply it to gatekeepers in the way foreseen by the DMA. This alignment between the DMA and GDPR would benefit both regimes and is an important step towards guaranteeing the effectiveness of the regulatory framework surrounding digital platforms.

**Acknowledgments.** The author would like to thank Eva Lachnit, Inge Graef, Cristiana Santos and the anonymous reviewer for their excellent comments on this paper.

**Competing interests.** The author declares none.