Kluwer Competition Law Blog

Fourth Workshop on the DMA – This is not a Blueprint for the DMA: The Unknown Knowns of Data-Reliant Business Models

Alba Ribera Martínez (Deputy Editor) (University Carlos III of Madrid, Spain) · Monday, May 8th, 2023

The DMA will start to apply on March 2024. Starting on the 2nd of May, the gatekeepers have a maximum of two months to notify their gatekeeper status to the European Commission (EC). The European Commission (EC) has acquired the compromise to make the process of the DMA's future implementation, monitoring and oversight of compliance as transparent as possible. After the first three stakeholders' workshops on the ban on self-preferencing and interoperability relating to messaging services as well as on the DMA's app store-related provisions, on 5th May, the EC held its fourth workshop regarding the regulatory instrument's data-related obligations.

This entry is the overview of the fourth workshop, which will be followed by other entries on the subsequent events the EC will hold during 2023 around the interpretation and discussion of the different provisions of the DMA. The outline of the first, second and third workshops may be found here, here and here.

Data-related obligations in the DMA

The fourth stakeholders' workshop held by the EC brought together a wide range of participants to talk about the present and future of data-reliant business models, namely the transformation that the DMA imposes on the way that the future-to-be-designated gatekeepers will unravel their business models since implementation day on.

To do that, the workshop handled the topic of data in relation to the regulatory instruments in three distinct panels fleshing out different approaches to how business and end users relate to the use, collection, processing, combining and cross-using of personal and non-personal data in their relations with Big Tech's operations. The first panel touched upon the self-enforcing prohibition under Article 5(2) of the DMA, which prohibits gatekeepers from cross-using, combining and processing personal data across their core platform services (CPS). The second panel alluded to the data-related obligations that will apply to those gatekeepers occupying a dual role within their own platforms with respect to the use of non-publicly available data in downstream markets, under the rule imposed by Article 6(2) of the DMA. Finally, the third panel of speakers brought forward the complexities arising from the application of Articles 6(9) and 6(10) of the DMA as regards the mandates of data portability of end-user data and the access of the data generated in the context of

the use of the relevant core platform services by the business users to the platform and the end users who have engaged with their products or services.

Tracking the data trail of gatekeepers across core platform services under Article 5(2)

The discussion around Article 5(2) of the DMA was interesting to watch and hear, insofar as it drove far off from the technical (or even legal) consequences of its effective implementation in the future. In principle, Article 5(2) of the DMA sets out an outright prohibition upon gatekeepers to cross-use, combine and process personal data across their core platform services.

Recital 36 establishes that the large number and deep data sets that the norm's addressees may access, as opposed to their competitors, provides them with a potential advantage in terms of accumulation of data, thereby raising barriers to entry to the digital arena. Therefore, the question raised by the text of the DMA is not one of proposing the reversal or prohibition of a business model, but that of levelling the playing field as far as data transformation activities are concerned.

Nonetheless, the provision is much more nuanced than that. On one side, Article 5(1)(d) provides that gatekeepers are also barred from signing in end users to their own services in order to combine personal data. In this regard, the regulatory instrument seeks to eliminate the well-known synching of different services and apps through the automatic signing-in of apps and services belonging to the same family of apps. For instance, the clearest example of the provision's implementation will bar Facebook from signing in a Facebook user into Instagram and combining the end user's personal data automatically.

On the other side, the interplay of the prohibitions set out in Article 5(2) with the GDPR's own provisions is nuanced but substantive. First, the prohibitions are pre-emptively exempted from applying if the gatekeeper manages to present the end user with the specific choice for opting into the processing, combining and cross-using of personal data across CPS'. However, consent is to be interpreted in the sense of Articles 4(11) and 7 of the GDPR, with the limitation that the gatekeeper does not request consent repeatedly (no more than once within a period of one year). Second, the prohibitions apply "*without prejudice*" to the possibility for the gatekeeper to rely on the legal basis set out in Articles 6(1)(c), (d) and (e) of the GDPR. This second limb of the provision follows the same direction as Recital 12, which expresses the regulation's wish to apply "*without prejudice*" to the rules resulting from other acts of Union law, such as the GDPR. In practice, this may imply that a gatekeeper may process and collect the same personal data alluded to in Article 5(2) DMA, but without the capacity of doing so throughout its core platform services. Against this preliminary backdrop, it does not seem that the "*without prejudice*" clause will be realised in practice, given that the GDPR's provisions may override the prohibition (as Konstatina Bania set out here).

Are privacy-enhancing business models a chimaera?

Instead of a fully-fledged exercise theorising about the implementation of Article 5(2) DMA, the debate was tainted with a moral and as-if backdrop to it, introduced by Carissa Véliz's main lines of reasoning (for reference, her highly-referenced Privacy is Power) questioning the base and foundation of the Big Tech business models: the ad-based business models.

In this regard, Véliz set out four main limbs to the thought-provoking panel: i) is the end user's consent to enable collection, combination and processing in the context of the gatekeeper's operations really to be regarded as a free choice?; ii) the importance of ending the trade of personal data, stemming from the fact that personal data are toxic assets which threaten the core of democracy (as seen in cases such as Cambridge Analytica or TikTok's threat to free press); iii) the moral significance of data creation; and iv) the importance of keeping track of data from the perspective of internal data management systems. The lineup of speakers took it upon themselves to pick up the gauntlet and follow the conversation in those terms but with the exception of Meta's representative in the workshop.

In general, the panel impinged the ad-business model based on the fallacy that data processing and collection are necessary for performing business in the digital arena. Instead, a large part of the panel urged advertisers and stakeholders to engage in the advertising market without the need to take recourse to data-intensive technologies. On the other side, however, a more diplomatic stance was exhibited by Meta's representative in the workshop who stressed the firm's capacity to both maintain its existing business model (especially through user profiling) alongside the compliance with the DMA's provisions. In a clear and straightforward, the representative put forward the firm's key ideas and design principles which are being considered and thought through at the firm level to deliver a meaningful and valid consent framework for the end user in the context of the prohibition. In this same sense, the to-be gatekeeper representative proposed that the optimal solution in terms of balancing out consent fatigue and providing the opportunity to the end user (still) to receive personalised ads and content would come in the form of an enhanced centralised centre, where consumer choice could be performed in degrees and across different services (a pair of allusions referred back to the FCO v. Facebook cases' remedies which are currently being discussed between Meta and the Bundeskartellamt, for some insight on the case and its current evolution, see here, here, here and here).

The data governance framework of the gatekeeper's internal data management systems

Moreover, a large segment of the panel was dedicated to the demarcation of core platform services as applied to the data-related operations performed by gatekeepers. Bearing in mind the Irish Council for Civil Liberties' voicing out concern on Meta's incapacity to know what data are collected, processed and used in their internal data management systems as well as where they lie within its great troves of data, a point was made on whether the implementation of Article 5(2) of the DMA will be feasible, at all (on the DMA's governance framework, see here).

If Article 5(2) of the DMA imposes the prohibition of performing these activities throughout the gatekeeper's CPS, to deem the provision applicable, one must at least know, three different items (aside from the basic and GDPR-related questions on whether personal data collection and processing is performed lawfully and legally, i.e., in line with one or more legal basis set out in Article 6 of the GDPR): i) what personal data belong to one CPS or to another one within the same organisational structure; ii) whether the data which are stored into the gatekeeper's data management systems are categorised and separated into personal and non-personal under the definitions provided by the GDPR (considering the Courts' current expansive approach in the field of data protection concerning the identifiaibility of individuals through their data, see here and here); and iii) whether the gatekeeper has the actual capacity to interrogate its internal data management systems in a way to bring them into compliance with the DMA, in light of the two

previous factors. The ICCL's concerns raised the answer that the regulatory instrument could not be adequately complied with due to this reason and the same reason was put forward in the first panel.

In light of the challenge, a range of speakers proposed to open up the gatekeeper's data processing activities entirely by forcing them to communicate and display their data processing records to the EC in order to bring them to compliance with Article 5(2) (and the GDPR!), whereas others proposed the EC to observe the compliance with the DMA by engaging in a regulatory dialogue (in principle, not permitted and not provided for provisions under Article 5 of the DMA).

An alternative look to this scenario was presented concerning the DMA's actual interpretation, i.e., what combination and cross-using mean in the context of the regulatory instrument. Aside from processing and collection (already defined in the GDPR), both concepts are left afoot as far as the prohibition under Article 5(2) of the DMA is concerned. On one hand, the scope of these activities could be circumscribed to the whole range of activities entailing the literal combination and cross-using of personal data. On the other hand, a narrower definition of these concepts could lead to considering necessarily those operations performed with reference to commercial purposes, but would not include those related activities including monitoring for fraud prevention and data security.

Even though, in principle, Article 5(2) of the DMA sets out the framework for a straightforward and outright prohibition over certain activities concerning the processing of personal data, future-proofing its implementation and effective enforcement is not as simple as could be expected, considering the leeway provided to transform the digital business models at large as well as the gatekeeper's inability to reign in their own data-related operations at large.

Data-siloing under Article 6(2) of the DMA

Similar to the prohibition set out under Article 5(2), the obligation imposed upon the gatekeeper by virtue of Article 6(2) of the DMA attempts to level the playing field with regard to the use of business user data in those scenarios where the gatekeeper occupies a dual role (as the platform holder and as a competitor in the downstream market vis-à-vis other business users). In particular, the prohibition seeks to silo data (i.e., to hinder the gatekeeper from leveraging that data in the context of its commercial activities) which proceeds from the business users' interactions with the platform in those relations where their competitive struggle unravels. By this same token, the prohibition seeks the long-run objective to build up end-user trust towards the platform.

Two main themes were unveiled throughout the panel: i) the provision's scope of application is; and ii) how the non-publicly available data requirement will be interpreted under the prohibition.

As opposed to Article 5(2), this provision cannot be interpreted in the light of the GDPR's definitions (i.e., personal or non-personal data), since the obligation is construed upon non-publicly available data which is ordered to be siloed for the gatekeeper. However, data siloing, as rightly pointed out by Prof. Giorgio Monti at the introduction of the panel, does not necessarily imply the separation of one dataset from another one, but that some data cannot be used by the gatekeeper regarding the development of particular functions, irrespective of the fact that the gatekeeper's actions shall be analysed as a whole (not limited to the business unit that competes with the business users of a CPS) (Recital 46 of the DMA).

In principle, both aggregated and non-aggregated data are covered by the prohibition as well as anonymised and personal data, as long as those pieces of data can be categorised under the broader concept of non-publicly available data. Following the reversal in the burden of intervention under Article 8 of the DMA against the gatekeeper, the requirements of the non-publicly available data will be sketched out by the norm's addressees, in the sense that they will have to demonstrate compliance in the negative.

From the technical perspective, compliance will be translated into data discovery and mapping, so that the European Commission (even via a designated monitoring trustee) can figure out how the data flows and systems work within the gatekeeper, in line with their content and the variety of dedicated uses to these data. Participants in the workshop affirmed that the GDPR compliance programmes are good indicators for future-proofing the effective enforcement of Article 6(2) of the DMA, namely by interrogating the gatekeeper's internal data systems through granular access controls and logs which demonstrate what data are used for what purpose, in line with the requirements of the regulatory instrument.

In Amazon's mind, however, the solution seems to be quite straightforward: the prohibition entails operating in the same way as they already committed to in their Buy Box and Amazon Marketplace cases before DG Comp in late 2022. In their opinion, the commitments covered in the realm of antitrust sufficiently comply with the requirements of Article 6(2) of the DMA, so that DMA-compliance will be extended as a look-alike to that prior sanctioning proceeding (as I already argued regarding the subject of overlaps in enforcement and the ne bis in idem principle, see here and here). In this same vein, Amazon's legal representative at the workshop established that the data covered by the prohibition would comprise both manual data (data that are collected and used by Amazon employers directly) as well as the data which are incorporated into the marketplace's processes in terms of commercial decision-making in the downstream market.

Building blocks towards data portability under Article 6(9) of the DMA (and not Article 20 of the GDPR)

In the last panel of the workshop, data portability under Article 6(9) of the DMA was discussed jointly with the data access obligations imposed on gatekeepers, which mirrors the obligation in Article 6(2) of the DMA. Once the non-publicly available data have been defined in terms of the latter provision, the data generated by the engagement of the business and end users in the platform shall be opened up to these same business users or third parties authorised by a business user (Article 6(10) of the DMA).

On the other hand, the enhanced data portability obligation imposed by Article 6(9) of the DMA will be more complicated to interpret, given its similarities with the same obligation imposed under Article 20 of the GDPR. The DMA provision extends the virtuality of the right recognised in favour of the data subject in the GDPR, given that it includes continuous and real-time access to such data. Throughout the panel, the speakers proposed to interpret both provisions coherently so that the exercise of Article 20 of the GDPR remains to be effective (although with a more limited scope as opposed to the DMA's enhanced right to data portability). In turn, previous experience in the realm of data protection may also set out the pre-conditions of the exercise of Article 6(9) of the DMA, stemming from the European Data Protection Board's (EDPB) interpretation of the provision via guidelines.

In this same vein, the next step for the effective enforcement of Article 6(9) of the DMA requires the cooperation and collaboration of the different authorities involved with the EC as the DMA's sole enforcer, notably with the EDPB as well as with the data protection supervisory authorities (DPAs) of the countries of the establishment of the gatekeeper.

Twofold paths were pointed out to open up the needed intra-authority collaboration concerning this particular provision: i) the day-to-day work and decision-making of the High-Level Group where the EDPB, European Data Protection Supervisor (EDPS) and DPA representatives may factor in their own experience (as provided by Article 40 of the DMA – the High-Level group was already established on March, see here for comment); ii) the issuing of common and additional guidelines jointly by the European Commission and EDPB for the interpretation of the right to data portability within the respective fields of law (whether a prior implementing regulation delegating this power on the EDPB as per Articles 46(1)(b) and (g) of the DMA is needed being uncertain).

Mirroring the prior experience of the exercise of the right to data portability under Article 20 of the GDPR also provides ample experience and space to rethink its 'enhanced' exercise under the DMA, from the technical perspective. Normally, the right to data portability is exercised by end-users in bulk through export-import APIs to port data from one service to another one (not directly through technical means). For instance, Google's service Takeout -launched in 2011, way before the GDPR's entry into force- is a good example of the technical means that have been deployed up until this moment to take Article 20 of the GDPR into practice (although concern has been recently voiced out in the Italian jurisdiction before the Autorità Garante della Concorrenza e del Mercato, due to a potential antitrust infringement by hindering the exercise of Article 20 of the GDPR in the downstream market). The use of APIs will still be of the essence in this context, despite that a clear and straightforward transposition of the requirements of a real-time and continuous exercise of this enhanced right to data portability was not proposed in the panel.

Key takeaways

As far as the DMA's data-related obligations go, two fundamental ideas must be considered when assessing the European Commission's future steps in delivering the promises of addressing the concerns around contestability and fairness in the digital arena:

- Although it may seem that way, the future-to-be-designated gatekeepers' data flows and internal data management systems must be thoroughly assessed in order to measure the effective enforcement of these provisions. Enforcement directed at scrutinising compliance with Articles 5(2), 6(2), 6(9) and 6(10) of the DMA will not be effective if performed from an outsider's perspective, given the primary concerns established regarding the gatekeeper's data governance structures in terms of administrability.
- The interplay between the DMA and the GDPR when applying these provisions will not be curtailed by Recital 12 (i.e., the 'without prejudice' clause'). Instead, DPAs, the EDPB and the EDPS will direct much of their attention (be that through the EC's instrument of choice within the regulatory instrument) to provide a coherent framework where data subjects -in the meaning of the GDPR-, as well as business and end users, can exercise their rights with ease and without undue interference.

Against this backdrop, much work is still to be done by the Commission in its efforts to provide a

robust legal framework to address the short and medium-term objectives of restoring contestability and fairness as well as the long-run aim to provide for a predictable foreground which may facilitate the emerging of privacy-preserving business models.

To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe here.

This entry was posted on Monday, May 8th, 2023 at 9:00 am and is filed under Data protection, Digital competition, Digital economy, Digital Markets Act, European Commission, Ex ante regulation, Online advertising, Online advertising restrictions, Online platforms, Platforms, Privacy, Regulation
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.