Kluwer Competition Law Blog

Full (Regulatory) Steam Ahead: Gatekeepers Issue the First Wave of DMA Compliance Reports

Alba Ribera Martínez (Deputy Editor) (University Carlos III of Madrid, Spain) · Monday, March 11th, 2024

The Digital Markets Act (DMA) is now applicable. Following the 6-month interim period where gatekeepers had the opportunity to adapt their business models to the regulation, the DMA now requires them to prove their effective compliance with its provisions. To do that, on 7 March 2024, the six designated gatekeepers in September (see here) presented their compliance reports and consumer profiling reports to demonstrate their efforts in satisfying the European Commission's expectations.

The milestone is only the starting point of the DMA saga that will follow during the coming months and years. As a consequence of the reversal of the burden of intervention, the six gatekeepers (Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft) have – preliminarily – played their part by submitting the two types of reports required under Articles 11 and 15 DMA. Starting in the wake of these submissions, the European Commission (EC) is now commended with the task of scrutinising and reviewing their technical implementation and interpretation of the DMA. The EC's assessment will factor into its analysis the contributions of interested stakeholders through the compliance workshops that it has already scheduled starting on 18 March spanning to the 26th where gatekeepers are invited to present these same solutions.

The blog post is particularly aimed at providing a high-level reaction to the gatekeepers' submissions, by remarking on their mishaps, omissions, and merit. As a preliminary note, one must note that the reports presented to the European Commission are quite idiosyncratic in nature. Some of them span through the DMA's interpretation over hundreds of pages, whereas others briefly sketch out the proposed plans that they had already leaked to the press in advance of the compliance deadline. At the time of writing, one must note that the six gatekeepers submitted their compliance reports, whereas ByteDance and Apple failed to present their consumer profiling reports abiding by the requirements under Article 15 DMA.

The DMA as a corpus of law: brief compliance reports vis-à-vis the extensive requirements under the regulatory templates

The DMA is not a standalone piece of regulation that must be interpreted and applied in isolation from any other rule. Over the last few months, the European Commission made a habit out of

passing regulatory templates expanding the scope and implications of the most substantial obligations engrained in the DMA, such as Articles 3, 11 and 15 (see here, here and here for comment on each one of them). This is the reason behind the fact that the DMA must be understood as a *corpus* of law, and not as a laundry list of provisions that must be enforced by gatekeepers, irrespective of any procedural and substantive limitations.

For drawing up their compliance reports, thus, the gatekeepers must follow the blueprint of the Template relating to Article 11 DMA. The Template requires them to explain in detail each one of the technical solutions that they propose to the European Commission with reference to a long list of items, for each one of the CPSs that were captured under designation and for each one of the provisions that they sought to comply with.

The form of compliance: short of narrowing down information asymmetries

Reality failed to deliver on the promise. In this regard, two sets of gatekeepers must be set apart from each other in terms of the form in which they presented their technical implementation of the DMA for 2024: i) those that did so exhaustively, such as Alphabet, ByteDance (to some extent), Meta and Microsoft; and ii) those that only presented a patchwork of marketing-approved statements to satisfy, in appearance, the requirement of submitting a compliance report, notably Amazon and Apple.

Even if one goes back to reading the compliance reports of the first group of gatekeepers, the narratives and technical implementations contained within them fall short of providing a deep understanding of how they will substantially comply with the DMA. At times, the compliance reports only remark on the proposed changes triggered by the regulatory templates in the fashion of a box-ticking exercise, irrespective of the fact that their implementation may raise more doubt than certainty for business and end users. In spite of the wide gap between each of the compliance strategies that the gatekeepers have proposed, there is nothing in the DMA imposing a form of implementation and it all boils down to the European Commission requiring additional information from the gatekeepers on how they intend to apply the DMA's provisions.

The only clear message that one can derive from the published compliance reports is that they do not provide nearly enough substantive technical details to determine with some degree of certainty if they comply with the DMA's provisions. Far from being trivial, this conclusion is of great consequence: stakeholders and third parties must play a major role in assessing effective compliance. The European Commission is the sole enforcer of the DMA, but that does not necessarily entail that it must perform its scrutiny in isolation.

The structure of the compliance reports: a three-step analysis

The DMA's provisions do not apply *en bloc* to all the twenty-two core platform services (CPSs) that remained captured by designation in September 2023. First, there are provisions that only apply to particular categories of CPSs, such as those directed at online search engines or online social networking services to impose FRAND access to their services under Articles 6(11) and 6(12). Thus, some CPSs (for instance, Meta's WhatsApp messaging service) are *de facto* excluded from complying with those provisions. Second, there is a second group of provisions that define

their scope of application in wider terms than those of the designated CPSs. For instance, Article 5(2) prohibits the combination of personal data from the relevant CPSs with personal data from third-party services or other services provided by the gatekeeper.

Additionally, on their compliance reports, gatekeepers have defended that they already comply with a great trove of the provisions contained in the DMA due to two main reasons, that boil down to i) the factual outset of the gatekeepers' business models; and ii) the interpretation of the DMA.

Regarding this first group of *de facto* compliance, for instance, Amazon puts forward on its compliance report that it does not apply most-favoured nation clauses – as prohibited under Article 5(3) of the DMA – "*on its Store-related contacts, program policies and other measures*", upon an extensive review of each one of them. In a similar vein, Meta also carried out an internal audit of its contractual agreements entered into with business users, the terms and conditions imposed on both business users and end users and any other informal practices carried out by the Meta teams. By doing that, it ascertained that, for instance, it already complied with the obligation contained under Article 6(13) requiring it to allow users to terminate their access to any of its CPSs without undue difficulty, given that users could "*terminate their accounts on Facebook, Instagram, Meta Business Suite, Meta Business Manager and WhatsApp rapidly and easily*". Before these types of statements, the European Commission can only but check those circumstances against reality, although it does not seem likely that the EC will trigger investigative measures as a first reaction to seek effective compliance.

On the note of the second tenet regarding the DMA's lack of application, the discussion that the gatekeepers engaged with in their compliance reports was much more substantive and nuanced. These are instances where the European Commission may demonstrate more action in terms of its scrutiny, insofar as the gatekeepers have not shied away from directly engaging with the interpretation of the DMA to disapply some of its more consequential provisions.

For instance, Meta has found no evidence in its business operations throughout its CPSs that the business user data being used by it would be "*in competition with*" Meta's business users. That is to say, Meta complies with Article 6(2) not only because it does not engage in that type of practice, but because it does not meet the requirement of being in direct competition with any other business user. The argument of 'less efficient competitors' that has loomed ever since *Post Danmark I* (Case C-209/10) seems to apply in the reverse so that Meta can declare its compliance with Article 6(2), albeit it has proposed a trove of (cosmetic) solutions to tackle its implementation.

Likewise, ByteDance's compliance report is quite salient in terms of how it justifies that TikTok already complies with the prohibitions under Article 5(2) DMA. As it already established on the designation decision of its TikTok service, ByteDance upholds that it does not "*offer a wide ecosystem of services similar to other designated platforms*" so "*the provisions of Article 5.2 are generally less relevant*". By this same token, ByteDance defends in detail that it is not forced to operate the prohibitions under Article 5(2) DMA insofar as "*TikTok's advertising services are an integral part of the TikTok entertainment platform*". Given that ByteDance's TikTok online social networking service encompasses all ByteDance's services, the gatekeeper establishes, that no processing of personal data for advertising services, combining or cross-using of personal data across proprietary services and to other CPSs applies. The argument would make sense if it were to enshrine the DMA reality, but one can already establish that does not seem to be the case for two fundamental reasons. On one side, ByteDance's designation decision (which has been appealed by the gatekeeper, see here and here) explicitly excludes TikTok's online advertising services from

the scope of its online social networking service (para 127 of the designation decision). In this regard, it is not entirely accurate to establish that TikTok's advertising services are an integral part of the TikTok overall platform, at least in the eyes of the DMA. On the other side, ByteDance notified the European Commission at the start of March (alongside Booking and X) that another of its services – potentially, its online advertising service – could fall within the scope of application of the DMA. Both the designation decision and the current developments, therefore, demonstrate that compliance with Article 5(2) on the side of ByteDance must prove to be more substantive in terms of technical implementation as opposed to the narrow-minded argument that the provision does not necessarily capture the platform's operations.

Proposed compliance on the most salient provisions: Articles 5(2), 6(9) and 6(10) DMA

Exhaustively reviewing each of the compliance reports presented by the gatekeepers would provide for a couple hundred pages of substantive analysis. Therefore, the post engages with those provisions that all the gatekeepers have substantively engaged with, given that they do not fall outside of the scope of compliance (be that due to *de facto* compliance or the gatekeepers' interpretation of the provisions described above). Those are the technical solutions proposed around the compliance with Articles 5(2), 6(9) and 6(10) DMA.

Article 5(2) DMA: choice screen-time, but what about the prima facie prohibition?

Article 5(2) prohibits the gatekeeper's leveraging of personal data across its ecosystem via different manifestations detailed within the four main strands of the provision listed under letters (a) to (d). Some of the gatekeepers, notably Alphabet and Microsoft, set forth different technical implementations for the different prohibitions engrained under Article 5(2) DMA, whereas Amazon, Apple, ByteDance and Meta submitted solutions that would transversally apply to all its CPSs. The common denominator of them all was that of the gatekeeper's interpretation of the provision.

Stemming from the gatekeeper's compliance reports, one would presume that Article 5(2) DMA provides great scope for leeway to include choice screens so that end users/consumers can consent to obtain personalised experiences on the gatekeeper's services. In fact, that is not entirely true, insofar as Article 5(2) establishes, *prima facie*, that the gatekeeper shall refrain from performing particular types of conduct, i.e., fundamentally, processing, combining and processing personal data across CPSs. However, the Union legislator included the possibility for the gatekeepers to display a choice screen to the end users so that they could grant their consent (in the terms of effective consent required by Articles 4(11) and 7 of the GDPR) to individually override the prohibitions.

So to speak, the gatekeepers began at the end of the provision by introducing choice screens allowing consumers to opt-in into the prohibited conduct (as I already set out in a recent paper). This was certainly the case for Amazon, which proposed two distinct prompts: the 'Store prompt' and the 'Ads Prompt'. The former will ask end users to grant consent for personalised experiences in Amazon's marketplace where performing that task would require Amazon to combine and use data from other services, such as Prime Video and Audible. The latter covers the end user's granting of consent to Amazon to use personal data from any Amazon service and third parties to

personalise the ads the platform shows across its interfaces. In a similar vein, ByteDance plans to tailor its video-editing tool CapCut to launch a slightly modified account-linking experience in the EEA in mid-March (aside from holding that most of the provision does not apply to it in terms of scope).

Bearing in mind this same perspective, Alphabet already started to roll out its implementation of the prohibition under Article 5(2)(b)-(c) DMA in January by asking users whether they wished to link their CPS services. Microsoft proposes a similar solution for its LinkedIn services, by displaying the consumer with a prompt asking whether he wishes to link the social network services. According to Alphabet's compliance report, the new consent framework required changes both at the front-end of Google's services – by providing users the opportunity to easily accept or reject relevant cross-service data exchanges – and in relation to its backend infrastructure so that the users' consent choices can be recorded and enforced across Google's systems. In principle, Alphabet's implementation entails that each CPS will operate as a separate data entity if the user decides to not grant consent to the linking of the services, whilst alternatively enabling the possibility to control the cross-service data flows. One might argue that the solution is not entirely coherent with the spirit of Article 5(2) since the prohibition should apply by default, and not as a consequence of the end user's decision to 'link out' the services. Once again, it all boils down to the European Commission's desire to defy Alphabet's technical solutions on their own terms. Alternatively, Alphabet adopted the compromise to work with advertisers and publishers who will gather consent for the processing of end user personal data to adopt compliance with the prohibition contained under Article 5(2) DMA of processing personal data, for the particular purpose of providing online advertising services, across with personal data of third parties that make use of the CPS.

Surprisingly, Apple's brief statement that it outright applied the prohibition by identifying cross-use and combination of personal data performed across its devices and completely ceasing in them is the closest solution of the gatekeepers to the underlying rationale of the provision. In a similar vein, Microsoft upheld that the provision did not apply to its Windows PC OS based on a detailed analysis of its processing and combining of personal data.

Furthermore, Meta put forward a chaotic proposal of solutions relating to its processing, combination and cross-using of personal data across its CPSs. This circumstance does not come as a surprise, bearing in mind the gatekeeper's iterations with data protection authorities relating to the legality of its data processing activities in the eyes of EU data protection regulation. Up to three types of different implementations apply across Meta's CPSs.

For Facebook and Instagram, Meta formulates three distinct types of remedies. First of all, Meta upholds its pay-or-OK model that it proposed in October 2023 which allows users to select whether they wish to consent to their personal data being processed (so that the social networks are funded in this manner) or whether they prefer to withhold their consent in exchange for a monthly subscription fee of EUR 10 ensures "*full and effective compliance with the DMA*". The same solution tangentially applies to Meta Ads' compliance with Article 5(2). Although it is true that the DMA applies, in line with Recital 12, without prejudice to the GDPR, Article 5(2) requires that end users are presented with a specific choice and given consent within the meaning of Article 4(11) and Article 7 GDPR (on the fallacy of the 'without prejudice' clause, see Bania here). Bearing in mind that data protection authorities have already voiced their concern around the legality of the pay-or-OK model against the benchmark of the GDPR, this first solution seems to fall amiss of, at least, 'full' compliance with the DMA. Second, Meta establishes that it already

complies with the provision on another distinct front, by providing the choice of consumers to consent to the combination and use of their personal data across Facebook and Instagram via the dedicated Accounts Centre that it introduced in June 2023 as a response to the German competition authority's case ordering the siloing of personal data per the platform's services. Third, Meta will display choice screens to provide users with the possibility to withhold their consent to combine their data across Meta's CPSs. It is yet unclear, however, how the pay-or-OK model will interact with this last solution, i.e., whether it will apply on top of it or whether the pay-or-OK model overrides the latter implementation. Regarding Facebook's processing, and despite that Facebook Dating and Gaming were said to be separate at the stage of the designation decision, Meta will also introduce an additional choice screen to enable users to consent to the combination of personal data across these complementary services with the social network.

In a similar vein, the European Commission's Meta designation decision bears a direct impact on compliance with Article 5(2). Given that the EC held in the designation decision that its messaging service (in the DMA's terms, number-independent interpersonal communication service) Messenger and its online intermediation service Marketplace are functionally distinct from the social network, then, the user will also be provided the choice to withhold its consent to combine its data across from Facebook to these CPSs. The remedy builds upon the artificial distinction of these services, that have forced Meta to provide a version of them as a standalone service. Although the solution makes more sense for Messenger, the fragmentation of Marketplace from Facebook is artificial, insofar as sellers and buyers will not be able to communicate directly to complete the purchase via Facebook's chat functionality. Instead, they will be forced to communicate via email.

Articles 6(9) and 6(10) DMA: APIs, third parties authorised by end and business users and requests for portability

Article 6(9) enshrines the gatekeeper's obligation to provide end users (and third parties authorised by them), at their request and free of charge, with effective portability of the data that they have provided or generated in the context of the use of a CPS. To do that, Article 6(9) establishes that they must cater to dedicated tools to facilitate the effective exercise of data portability, including the provision of continuous and real-time access to such data. Article 6(9) turbo-charges the right to data portability already contained under Article 20 GDPR by enhancing the conditions in which the right must be exercised, notably via the provision of continuous and real-time access to such data. A similar obligation applies under Article 6(10) DMA concerning the data that business users generate in the context of their use of the CPSs. In this latter instance, however, the gatekeepers are forced to provide effective, high-quality, continuous, and real-time access to, and use of, aggregated and non-aggregated data.

One would have expected the solution to be APIs (Application Programming Interfaces). In other words, gatekeepers are expected to incorporate code that enables services to communicate with each other. In this particular case, the gatekeeper's services with the services of third parties may wish to leverage that same data generated in the context of CPSs for catering services in the market, in line with the contestability goal engrained under the DMA. Most gatekeepers delivered on the promise, although the European Commission will be forced in the coming months to consider whether they fulfil the requirements of continuous and real-time required by both provisions.

On the side of compliance with Article 6(9) DMA, most gatekeepers have adopted an active stance. For instance, Alphabet proposed to introduce its Data Portability API which will enable users to authorise third-party services directly so that they can export data into their own services. The process, however, will only be actioned if the third-party developer is previously verified by Google and if it makes accurate representations about its access to and use of the end user's data. The implementation will hardly represent real-time and continuous access to the data, insofar as Google will require a fresh authorisation for each data portability request that is formulated to "*ensure sufficient user choice and control*". Alphabet establishes, however, that the alternative for the user is to continue using its portability tool Takeout by transferring data directly to the selected third-party cloud storage services directly from the Takeout user interface.

Furthermore, ByteDance outlined the detailed solution that it has designed to enable data portability in the terms of Article 6(9) by introducing its Data Portability API, which allows third parties to integrate with its service. As opposed to Alphabet's implementation, ByteDance's access to its Data Portability API may operate through a single data portability request (for a one-off porting of the end user's relevant data) or through a recurring request that the end user may establish to enable the developer to make repeated requests over time. Alternatively, ByteDance has already enhanced the functionality of its Download Your Data service by improving its data access speeds and offering a more granular selection of the data that can be ported by the end user. In a similar vein, Microsoft declared it would introduce a free-of-charge API (the Member Data Portability API) and supporting programs to enable members of LinkedIn or third parties authorised by those members to access their data. The authorisation tokens granted by the end users will be valid for one year and access to the data will be unfettered unless the end user chooses to terminate access earlier. Microsoft even provides an approximate timeframe of how long it will take the Member Data Portability API to retrieve the data, namely 10 minutes for the first API call for some data types and up to 48 hours for other data types.

Other gatekeepers proposed similar solutions to comply with Article 6(9) but did not provide much detail on how those tools would operate in practice. For instance, Amazon proposed the introduction of an API designed to share data with authorised third parties (the Portability API) and an additional self-service download portal accessible by the end users (the 'Transfer Your Data' portal). Moreover, Meta proposed to increase the recurrence of its existing portability tool Transfer Your Information from a monthly transfer of data to a daily transfer and has expanded the capacity of its Download Your Information tool to enable all data available for download to be transferred directly to third-party storage destinations like Dropbox. Similarly, Apple briefly remarked on the fact that it will provide users with the ability to export their personal App Store data to authorised third parties. However, it delayed compliance of further portability implementation for the fall of 2025 when it provides adequate solutions to help mobile operating system providers transfer data from iPhone to non-iOS phones and for late 2024/early 2025 when it will enable dedicated processes to enable the exporting and importing of relevant browser data into another browser on the same device.

On the side of compliance with Article 6(10) DMA, gatekeepers have focused their solutions on a passive approach. By this token, Alphabet and Microsoft submitted that they would monitor the data they receive from business users so that they can, perhaps, expand the types of data that they make available to them. Amazon and Meta set forth that they would introduce dedicated processes for facilitating data flows (through the End User Data Access API for Amazon's case) in those cases where their existing tools did not provide for such data. ByteDance and Apple did not submit any technical solutions to the end of complying with the provision.

Intense scrutiny expected on many fronts – first round: #FreeFortnite

Against the background of the brief review of the DMA's technical implementation presented by the gatekeepers on their first round of compliance reports and the form in which they have done so, a vast array of questions and unknowns still loom over the European Commission's expected enforcement.

At this stage of the post, an avid reader would ask: and what about Apple? A few weeks back, Apple issued an announcement that it already formulated the all-encompassing changes that it would apply at the European level as a consequence of the DMA's application (for a comment on them, see here). The press release faced great backlash from app developers currently operating on the App Store. The most salient omission that one notices when reading Apple's compliance report is that of its free structure. In appearance, Apple's re-modelling of the way in which it would cross-subsidise its ecosystem has completely vanished into thin air.

In parallel to Apple's statement, Epic announced that it would release its own alternative app marketplace for gaming, the Epic Games Store. To that end, Epic received its Apple Developer Account via its affiliate Epic Games Sweden AB. Three days in advance of the DMA compliance deadline, Apple terminated this same developer account. Effectively, the move meant the direct exclusion of Epic Games Store from iOS devices. The most surprising part of the exchanges between Apple and Epic is not that of the direct exclusion but of its final resolution. As Thierry Breton announced on 8 March 2024, Apple had reinstated Epic's developer account and declared that "*from Day 2, (the) DMA is already showing very concrete results!*".

In my own mind, however, the correlation between the outright exclusion of a competitor from catering services on one's proprietary ecosystem and the DMA's mechanisms does not seem to be so straightforward. Let's think about the counterfactual in enforcement: if DG COMP/DG Connect were to apply the DMA to resolve the row between Epic and Apple, then, what provision and procedure would have it applied? The answer is not completely evident if one engages with the DMA's text on its own merits, especially if one bears in mind that exclusionary abuses are parcel and part of the enforcement under Article 102 TFEU. The first of the DMA's victories (to free Fortnite on iOS devices, as Breton tweeted), thus, seems to come out more from the political and institutional pressure that the EC will be able to exert over gatekeepers than from the legal and procedural intricacy of the regulatory instrument.

Moreover, a wide range of surprises truffle the compliance reports submitted by the gatekeepers, and the European Commission will have to deeply scrutinise them so as to call foul in case they fall below the threshold of effective compliance. For instance, this may well be the case for Alphabet's proposed solution to comply with the anti-steering obligation contained under Article 5(4) DMA for Google Play. The gatekeeper has introduced the option for Google Play developers to promote offers within their Google Play apps and show hyperlinks that take users to external sites to conclude contracts for those offers. However, the technical implementation works on the premise that developers sign up for the External Offers program, which makes authorisation conditional on the acceptance of a new fee model imposed on these developers.

In those instances where gatekeepers must open their digital ecosystems to third parties and alternative services, the general trend is that the ecosystem holders are not prone to relinquish full

control of the operations that are completed on their devices and services. By doing so, the DMA's application may result in transferring the questions arising around contestability and fairness concerns to the verification and authorisation processes that the gatekeepers may legitimately implement to protect their own commercial interests. Thus, the DMA enforcement may, in the end, result in an empty promise of openness.

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, March 11th, 2024 at 9:00 am and is filed under Amazon, App stores, Apple, Apps, Digital competition, Digital economy, Digital markets, Digital Markets Act, Europe, European Commission, Ex ante regulation, Facebook, Google
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.