Kluwer Competition Law Blog

Meta's DMA Compliance Workshop – The Power of No: Making Perfectly Rational Choices

Alba Ribera Martínez (Deputy Editor) (University Carlos III of Madrid, Spain) · Wednesday, March 20th, 2024

The Digital Markets Act (DMA) became entirely applicable on 7 March 2024. By then, the gatekeepers issued their compliance reports documenting their technical solutions and implementation of the DMA's provisions under Article 11 DMA as well as their reports on consumer profiling techniques as required under Article 15 DMA (see here).

I will be covering the workshops organised by the European Commission per each of the gatekeepers under The Power of No series, where the representatives of the undertakings meet with stakeholders to grind their compliance strategies and solutions. This blog post covers the second workshop organised by the EC for assessing Meta's compliance solutions, find here the review of the first workshop relating to Apple's technical implementation of the DMA.

The clash between the governance structures and models of European regulation

For Meta, compliance with the DMA is not only about strictly complying with the regulation's provisions and fighting those instances where they disagree with the European Commission tooth and nail. According to the gatekeeper, the interweaving and interacting pieces of regulation that the European Union has recently passed as a consequence of its digital strategy frame a significant rule book of mandates and prescriptions that present conflicting principles, which are backed by unique governance structures and models. The most evident clash between these substantive pieces of regulation, for the undertaking's particular case, is that concerning the DMA with the GDPR. This is precisely the cornerstone of Meta's narrative around its compliance with the regulatory framework.

Meta's star compliance solution is that of presenting users with up to six different consent moments across the user experience of all of their services. The avid reader of this recap of the EC's workshop will immediately think: Meta's pay-or-OK subscription model, right? Well, yes. The high stakes of Meta's compliance plans towards resolving the need for effective enforcement under the DMA derive from the original idea that the Court of Justice first pointed out in July last year (see for review on Case C-252/21) that Meta could produce an equivalent alternative for catering its product online where processing operations are not performed at such a large scale or even at all, albeit that users would have to correspond with an appropriate fee to cover for the

service's value. In this sense, Meta's compliance report and solutions, which specifically relate to how it processes data and the data-related obligations engrained into regulation revolve around this model, proposed by the gatekeeper last year in the EU.

Aside from Meta's implementation of WhatsApp's interoperability obligation as a number-independent interpersonal communication service provider under Article 7, the EC's compliance workshop extensively considered Meta's technical implementation of how it processes, combines and uses data across its core platform services (CPSs). Thus, the blog post will first consider Meta's consent moments as stemming from its interpretation of the prohibition set out under Article 5(2) to then analyse the gatekeeper's efforts to comply with its ad transparency obligations (namely Articles 5(9), 5(10) and 6(8) of the DMA) and its data portability obligations with reference to end and business users (correspondingly, covered by Articles 6(9) and 6(10). Finally, the piece briefly explores the undertaking's implementation of Article 6(2) relating to the prohibition of using non-public data across services where it is in competition with business users as well as the FRAND conditions of access mandate under Article 6(12).

More consent moments and separate products: more choice?

Meta set out its compliance with Article 5(2) by highlighting that it now displays up to six different consent moments on its services to comply with the provision. Article 5(2) prohibits the gatekeeper from combining, processing and cross-using personal data across its CPSs. Its approach towards overriding the prohibition, however, is fragmented from the perspective of its designated CPSs (see a comment on the designation decisions here). Different solutions apply, in principle, to the distinct services catered by Meta to its end users.

Facebook and Instagram: pay-or-OK consent model and Accounts Centre

Meta streamlines its pay-or-OK model as a solution to achieving effective compliance with the DMA regarding these CPSs. The pay-or-OK model consists of presenting the end user (one could say, in translating the terms to EU data protection regulation, the data subject) with a choice in fine-tuning its data protection preferences. On one side, the end user may prefer to continue to use Meta's social networks as is, meaning that those services are subsidised for the user and provided for free. That choice is based on the assumption that Facebook and/or Instagram will heavily rely on the processing of personal to perform personalised online advertising.

On the other side, the end user may prefer to benefit from a 'no ads' experience on Facebook and/or Instagram in exchange for a subscription fee. Originally, that fee was EUR 9,99 (plus the additional commission fee charged on smartphones if the user was to perform the choice on iOS or Android, EUR 12,99), whereas in discussions with EU data protection authorities that fee will be possibly lowered to EUR 5,99, as confirmed by Meta's legal representatives in the workshop. If the user chooses this second option, that does not mean that every single type of personalisation will be eliminated from the service, but that personalisation will not be based on the end user's engagement for the particular purpose of online advertising.

Although the pay-or-OK model was proposed long after the German competition authority's case against Facebook was resolved, the technical deployment of those prompts directed at users takes

place through the dedicated solution that Meta came up with to comply with the Bundeskartellamt's requirements to imprint the siloing of data: the Accounts Centre. In principle, the Accounts Centre was a way for users to keep their Facebook and Instagram data separate from each other. However, the pay-or-OK model has now permeated the functionality to allow users to choose with respect to an ads-based or a non-ads-based experience. In this particular sense, the end user is not only provided with the sole opportunity to decide to pay for being protected in terms of the processing of personal data for the purpose of advertising across Meta's social networks, but the end user can also pick and choose what services it wants the pay-or-OK model to apply to. Therefore, the end user may choose to subscribe to the pay for a 'no ads' experience on Facebook whilst navigating on Instagram via the traditional operations of Meta's processing operations. One must say that each additional account that the end user adds to the 'no ads' experience will account for an additional EUR 6,00.

Asked by participants within the workshops on whether the no-ads-based subscription user experience enjoyed in exchange for a fee amounting to EUR 120 a year was, in fact, an equivalent service to the catering of the service through the processing and combination of data, Meta's representative was crystal clear in elucidating the strength of the model that they are presenting to its end users. In Meta's own words, it is offering quite a low price based on the subscription models of its peers, notably the X Premium subscription for EUR 9,60 or the YouTube Premium subscription for EUR 11,99.

For those cases where end users already made their choices prior to the compliance deadline of the DMA (given that the subscription model was already rolled out last year) leading to an ads-based user experience, then an additional prompt will also be displayed so that the end user confirms whether she wants to override the prohibition under Article 5(2) DMA. In these cases, Meta will interpret that the user's affirmative action in confirming its willingness to base its own experience on personalisation and cross-subsidisation based on online advertising is effective consent in the sense of Articles 4(11) and 7 GDPR to override the mandate. Alternatively, when the end user has chosen the subscription model, then Meta confirms that it would respect the choice without the need for an additional prompt to confirm the choice, despite that if the end user then switches back to the ads-based experience, then Meta will start to operate again, in the fashion of clean slate start, based on its processing of the end user's engagement throughout the service.

Messenger, Marketplace (Gaming and Play): separate CPSs, so separate user interaction

Meta's designation decision issued last September by the European Commission is key to understanding the gatekeeper's second set of technical solutions relating to compliance with Article 5(2) DMA. In its designation decision, the EC decided to segment and separate Facebook Marketplace as an online intermediation service as well as Messenger as a number-independent interpersonal communications service (NIICS) from its social networking service Facebook. This was particularly surprising for some, including myself, insofar as the delineation of distinct services meant that complementary services embedded within Facebook were artificially disgorged from it. Moreover, the European Commission applied the same type of analysis to Facebook Gaming Play and Dating to consider whether they would also be held as distinct CPSs in the eyes of the DMA. The EC decided against it and held that they should remain within the remit of the social network CPS.

Bearing in mind this separation, the natural consequence of that policy choice was to provide end users with the possibility to access those services separately. Therefore, for instance, Meta has provided the possibility to access Messenger (which was formerly the social network's chat functionality) without having to register on Facebook. In parallel, Facebook has incorporated an additional chat functionality which holds separate from Messenger. By doing that, in Meta's view, data combination is not operated across those CPSs, insofar as consumers can withhold their consent for that particular purpose. The immediate consequence of that choice is that, in reality, consumers will start a new experience afresh exclusively on Messenger. The same choice and consumer flow have been incorporated into Facebook Marketplace. Functionality solely embedded on Facebook will, thus, not be catered to Messenger and Marketplace end users, such as Facebook's stories or the ability for sellers to message buyers directly on Facebook's functionality (and they will have to do so via a dedicated emailing functionality that the gatekeeper will roll out).

A completely different solution may apply, however, to Facebook's Gaming and Dating services. Although the EC initially categorised them inside of Facebook's CPS, Meta interprets that it designated them as 'other services' and as such it should provide a solution akin to that established for Messenger and Marketplace. That is to say, for example, that Meta is forced by the DMA to separate the gaming experience functionality on Facebook Gaming from the social network. Despite that the gaming feature is mainly centred on social gaming experience (that is, gaming based on the interaction with Facebook friends), Meta interprets that Gaming should, instead, be disgorged to a point where non-social gaming experiences can be also sourced via these means. Meta did, however, not go into the technical details that would support the choice nor on the fact of whether the implementation would be feasible, insofar as games for Facebook Gaming are exclusively developed by third parties and not directly by Meta.

Data portability: what is the point, if not to foster contestability?

Meta's technical implementation of the provisions relating to its obligation to cater for more transparency relating to its intervention within the ad tech stack (under Articles 5(9), 5(10) and 6(8) of the DMA) was quite straightforward and built upon the gatekeeper's already existing reports on the same matters. In that particular regard, Meta clearly differentiated its owned and operated (O&O) activities from those processing activities that it performs across its Audience Network (that is, via the selling of ads via third-party websites with which they are associated via this network). On the side of O&O, Meta held that advertisers can already see what they are charged when displaying their ads directly on the gatekeeper's services, such as Facebook or Instagram. According to the undertaking, these activities are the bulk of Meta's activities relating to advertising.

On the side of Meta's Audience Network and how they interact with advertisers and publishers on that side of the market, the gatekeeper set forward that it had introduced a DMA-specific report that works in two distinct directions. First, Meta will start displaying for advertisers on Ads Manager an additional report detailing what Meta pays to Audience Network publishers when their ads are displayed there. Second, Meta will also publish and update a report of the same kind on Monetisation Manager, notably remarking on the price information that the advertiser invested in so that its ad would be displayed on the third-party website. In response to several questions asked by the participants of the workshop, Meta went into more detail on the level of granularity of the data that is available to both advertisers and publishers, which could be further broken down by

geography, placement, and date.

Staying on the topic of business users, Meta also detailed its implementation of Article 6(10), which follows from its already existing policy of sharing valuable insights with them via Meta Business Suite and the dedicated dashboards for each one of its social networks. Against the background of the comprehensive nature of the information already available to business users, Meta has fundamentally created *ex-professo* for the occasion of the DMA a dedicated request process form through which business users can make requests on information that is not already available through the existing tools.

Moving forward to the end user perspective, however, Meta faced a bit more backlash from stakeholders participating in the workshop. Throughout its speech, Meta put forward its previous efforts (pre-DMA) in catering to data portability through its two dedicated systems: Download Your Information (DYI) -which was launched over a decade ago and provided for data portability in a wide-spanning manner- and Transfer Your Information (TYI), launched in 2020 and catering to the portability of photos and videos on Meta's social networks. Building upon both existing tools, Meta has substantially expanded their scope and functionality. First, DYI has been substantially expanded to enable the downloading and transferring of all available data on Meta's CPSs. Second, both DYI and TYI have introduced the option for regular transfers (even on a daily basis for TYI) of information so that even automatic recurring downloads and transfers may be performed during a span of up to 12 months with a single authorisation from an end user to a third-party service provider. Third, both of those tools are also expanded to cover the (artificially segmented) Messenger and Marketplace services and the information that the end user may embed within them as a consequence of the standalone use. Fourth, Meta has decided to cater to these tools in the realm of the EU but also on a global basis to all of its worldwide users.

It all seems perfectly normal and compliant with the DMA, for now. However, the tenet that stakeholders stressed within their responses and questions to Meta's compliance plan around Article 6(9) was that those data portability cannot be made available to third-party service providers directly so that they can cater new products and services as a consequence of their direct porting of data. Instead, both DYI and TYI only allow the end user to port data across ten third-party destinations, such as Dropbox or Google Drive. One would, thus, assume that if the end user wished to port data across to a third-party (competitor) service, then it would have to first port it through one of these authorised third-party destinations to then pass it on to the third-party service provider. Even though Meta was repeatedly asked about the criteria, processes or solutions that it could implement to expand on the third-party destinations that are currently available on its portability tools, it did not respond to any particular solution.

I'll trust you for your word: use of non-public business user data and FRAND conditions of access

The third panel within the workshop was, too, quite straightforward to grasp and did not raise much suspicion amongst the participants. As a response to previous criticism relating to its use of business user data in the context of its Marketplace coming from antitrust scrutiny from the EC and the UK's CMA, Meta held that it was in a position to assert that it does not use any business-user generated data across its Meta Ads in competition with those same business users. Alternatively, it also highlighted that within the value exchange between Meta and its business users relating to

online advertising (those are, advertisers), advertisers contribute a minute volume of data as opposed to data made available by Meta. In any case, if Meta was to be stripped of this small volume of data, it would not be able to deliver its advertising services for its advertisers on its O&O inventory or through its Meta Audience Network.

Although Article 6(2) does not exclusively apply to Meta's use of business user data for its Meta Ads CPS, the gatekeeper did not provide much detail on whether such use of data was performed across the rest of its CPSs, since the risk assessments that it had performed related to this matter in isolation.

Turning to the obligation to provide access for business users to its social networks in FRAND terms, Meta briefly outlined how its current terms and guidelines meet those requirements. For instance, the gatekeeper held that end users and business users' accounts would only be suspended due to violations of the terms already presented to them when they registered into the service. Implementation revolved, in this respect, on defending that its current terms stayed within the limits of what the FRAND yardstick allows for. Furthermore, Meta also detailed that it introduced an alternative dispute mechanism to allow Facebook and Instagram business users, as defined via the DMA, to challenge the application of those same conditions of access in charge of a dedicated review board subject to the elements of independence and impartiality.

The WhatsApp interoperability solution: a long way ahead

One of the most striking and impactful shifts that the DMA operates is that of NIICS interoperability under Article 7 DMA. Only two services of the gatekeepers have been designated, across the board, as NIICS: Meta's WhatsApp and Messenger. At the start of the workshop, Meta confirmed that a technical solution will be shortly proposed for Messenger. However, Meta only set forth its implementation for WhatsApp's messaging services.

Prior to the implementation solution, Article 7 binds the gatekeeper to publish a reference offer laying down the technical details and general terms and conditions for the interoperability with its NIICS to take place with a third-party NIICS. Meta has already released its reference offer by briefly detailing how those details will work in practice. In any case, Meta's representative went through those items in turn. As Meta pointed out, it set out in its reference offer two different approaches toward interoperability: the client-server infrastructure and or the proxy server approaches. The client-server infrastructure means that WhatsApp remains in control of messaging, despite giving way to third-party NIICS to interoperate. Third parties will directly embed that protocol per each of the end users that would opt in to interoperability. In other words, WhatsApp would route the messages to the intended recipients whilst clients in third-party NIICS would send messages directly to WhatsApp's server via interoperability.

As opposed to this solution, where WhatsApp would remain in full control of interoperability, the gatekeeper also proposed an alternative for third-party NIICS to place a proxy server in between the WhatsApp service and the third party. This second approach will impair WhatsApp from running integrity checks to ensure the highest standard of security, Meta argued, but it was making great efforts to preserve the same level of protection for its service.

In terms of security, WhatsApp has relied on the Signal protocol since 2016 for all of its messages and calls and both of its interoperability solutions rely on this protocol because it is the industry-

leading standard for messaging services. However, to facilitate further interoperability implementation, WhatsApp will also offer a range of solutions for third parties, including that they can build upon the open-source version of this protocol, they can directly negotiate their license with the Signal foundation or they can sub-license directly third-party NIICS free of charge. Moreover, in response to the feedback obtained from both the European Commission and the third parties, Meta will also consider the interoperability requests from third-party NIICS with compatible encryption protocols that provide the same level of security. By its very nature, the interoperability solution means, in terms of security, that WhatsApp will no longer guarantee that anyone other than the recipient and sender of messages will be able to access those communications, as it did until this moment.

From the perspective of the end user, WhatsApp will now display a separate tab for its third-party chats and will require users to opt into interoperability if they wish to do so. Although Meta did not advance any concrete details, it did acknowledge that users would be able to select the third-party NIICS that it would want to operate with. That is to say, an interoperability request from a third-party NIICS to WhatsApp does not complete the whole process. Instead, the user will have to opt in (up to twice) to receive messages originally sent from alternative NIICS providers.

Against the framework of this reference offer, therefore, third-party NIICS have directed interoperability requests to Meta and now it is undertaking the evaluation of those requests so as to then launch implementation in the coming three months.

Key takeaways

Meta’s intervention in the EC’s compliance workshop was both constructive and eventful. The gatekeeper did not highlight the risks of the regulation but rather the opportunities that it opens up to enhance contestability in the market. Although it is undeniable that Meta’s compliance plan is not without its faults and red lines, it presents a comprehensible account of the expected steps that the undertaking will have to make in the coming months and years.

As Meta’s representative pointed out in his first presentation to the workshop, the most salient (and conflicting) provision that the EC is bound to monitor with regard to its enforcement is that of Article 5(2) which does not neatly fall within the definition of a ‘self-executing’ obligation, i.e., easy to grasp and straightforward to interpret. Instead, the provision should have fallen within the scope of those obligations subject to specification by applying Articles 6 and 8 DMA. The ‘prejudiced’ interplay (despite the content of Recital 12) between the DMA, the GDPR and other pieces of EU regulation will deliver on how compliance will be resolved and accounted for under the DMA. All in all, Meta’s compliance solutions cover loads of common ground that the Commission may agree on, but it also leaves ample missing gaps that must be sustained and completed with effective enforcement in interpreting the regulation’s spirit.

---

please subscribe here.

Kluwer Competition Law

The **2022 Future Ready Lawyer survey** showed that 79% of lawyers are coping with increased volume & complexity of information. Kluwer Competition Law enables you to make more informed decisions, more quickly from every preferred location. Are you, as a competition lawyer, ready for the future?

Learn how **Kluwer Competition Law** can support you.

This entry was posted on Wednesday, March 20th, 2024 at 8:30 am and is filed under Advertising, Data protection, Designation Decision, Digital, Digital competition, Digital markets, Digital Markets Act, Facebook
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.