The European Court of Justice in *Meta Platforms* leaves competition and data protection authorities with an assignment

*By Inge Graef*

Competition authorities can identify a violation of the data protection rules when such a finding is necessary to establish an abuse of dominance under the competition rules. This is the main outcome of the judgment that the Court delivered in *Meta Platforms* on 4 July 2023. The judgment is the next step in the saga that started with the 2019 competition decision of the Bundeskartellamt (the German Federal Cartel Office) requiring Facebook (now Meta) to refrain from combining user data from different sources beyond its social network. The judgment provides a welcome confirmation that data protection standards can also matter for the interpretation of the competition rules. However, what is more remarkable and less expected is the general framework the Court sets out for coordination between competition and data protection authorities building on the duty of sincere cooperation and the clarity with which it evaluates the different legal bases Meta invoked for processing user data. The judgment can become a reference point for assessing the legality of personal data processing by dominant firms, but also leaves competition and data protection authorities with an assignment to explore how to coordinate their work in the future.
From German to EU competition law

Because of the controversy about integrating data protection rules into competition analysis at the time of the decision, the Bundeskartellamt was careful to frame its concerns in the context of German and not EU competition law. The German Federal Court of Justice held in cases like *VBL-Gegenwart* and *Pechstein* that the German prohibition of abuse of dominance in Section 19(1) of the ‘*Gesetz gegen Wettbewerbsbeschränkungen*’ (GWB) can also be invoked in cases where one party dictates contractual terms that breach civil law principles or constitutionally protected rights. Following this approach, for which no precedent exists at EU level, the Bundeskartellamt relied on the *General Data Protection Regulation* (GDPR) to hold Meta liable under German competition law for exploiting its dominance by imposing unfair terms and conditions on users.

At the heart of the case was the Bundeskartellamt’s finding that Meta, as a dominant firm, made the use of its social network dependent on users agreeing in the terms and conditions to the combination of data collected through Meta's different services beyond its social network and from third-party sources. According to the Bundeskartellamt, Meta did not have a valid legal basis under the GDPR for this form of data processing and thereby engaged in an exploitative abuse under Section 19(1) GWB. The Higher Regional Court in Düsseldorf had ruled in favour of Meta in interim proceedings—arguing in its *August 2019 judgment* that the Bundeskartellamt was exclusively discussing a data protection and not a competition problem. However, the German Federal Court of Justice on appeal sided with the Bundeskartellamt in qualifying Meta's conduct as abusive in its *June 2020 judgment*.

The case came to the EU level via a *preliminary reference to the Court* from the Higher Regional Court in Düsseldorf in the proceedings on the merits. The Düsseldorf Court asked the Court, among other things, whether a national competition authority can make findings about the consistency of personal data processing with the GDPR in the course of an abuse of dominance investigation under competition law. The Court answered this question in the context of the abuse of dominance prohibition of Article 102 of the Treaty
on the Functioning of the European Union (TFEU), thereby bringing the case within the remit of EU competition law.

**Data protection concepts impact competition law, but less so the other way around?**

The Court is clear in confirming the ability of national competition authorities to check the consistency of personal data processing with the GDPR where relevant to assess abuse of dominance. While acknowledging that data protection and competition authorities have different functions and tasks, the Court notes that there is no provision in the GDPR preventing national competition authorities from finding a violation of the GDPR in the performance of their duties (paras 43-44). In the view of the Court, the compliance of conduct with the GDPR may be *a vital clue among the relevant circumstances of the case* in order to establish whether that conduct meets the competition rules (para. 47). According to the Court, access to personal data has become a significant parameter of competition in the digital economy. Therefore, excluding the GDPR rules from the legal framework to be considered by competition authorities in abuse of dominance cases *would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union* (para. 51).

Considering the earlier controversy about the relevance of data protection rules for competition law, these statements of the Court may seem striking. However, judgments like *AstraZeneca* and *Allianz Hungaria* already recognized that the breach of an area of law can be a factor in determining a violation of competition law as well. It is therefore no real surprise that the Court confirms that competition authorities can look towards data protection law when conducting competition investigations. While the reference to the need to prevent competition law’s effectiveness being undermined is a phrase that the Court uses more often to support an expansive interpretation of the competition rules, the strong language is nevertheless noteworthy. The Court almost presents it as a stated fact that data protection concepts influence competition law.

The Court is less unequivocal about whether competition concepts matter for data protection law. As Advocate General Rantos also pointed out in his Opinion, the Court argues that the dominance of a social network provider must be taken into account in
determining whether a user has validly and freely given consent but does not, as such, render consent invalid (paras 147-148). Following this nuanced position, the Court does express serious doubts about whether the consent of Facebook users can be considered freely given. The Court notes that Article 7(4) GDPR requires users to be free to refuse consent for data processing activities that are not necessary for the performance of a contract and that the processing at stake does not appear to meet this threshold (para. 149).

Given the scale of the data processing and its significant impact on Facebook users, the Court also submits that it is appropriate to give users the possibility of giving separate consent for the processing of data within the Facebook social network and for the off-Facebook data. In the absence of such a possibility, the consent of users to the processing of off-Facebook data must be presumed not to be freely given in the view of the Court (para. 151). Finally, the Court stipulates that users must still be able to use the social network if they refuse consent for data processing activities that are not necessary for the performance of the contract. According to the Court, this means that users have to be offered an equivalent alternative not accompanied by such data processing operations – if necessary, for an appropriate fee (para. 150). The same requirement can be found in the context of the provisions regarding the combination of personal data in Article 5(2) of the Digital Markets Act (DMA), which are based on the Bundeskartellamt’s case against Meta. According to recital 36 to the DMA, to prevent gatekeepers from unfairly undermining the contestability of core platform services, end users need to be offered a less personalized but equivalent alternative, without making the use of a core platform service or certain of its functionalities conditional upon consent.

While stating that the dominance of a data controller does not by itself prevent users from giving valid consent, the Court’s detailed stipulations do substantially limit the circumstances in which a dominant firm can demonstrate that it has obtained valid consent. Where personal data is combined across services, it seems that consent can only still be regarded as valid when users can separately provide or refuse consent for any processing that is not strictly necessary for the performance of a contract. This clarification
by the Court considerably restricts the ability of providers of digital ecosystems like Meta to combine personal data from different sources and between different services.

**Data processing by a dominant firm**

Beyond its strict interpretation of consent, the Court also approaches the other legal bases for personal data processing under the GDPR strictly. For determining the necessity of data processing for the performance of a contract, the Court lays down a standard of data processing being ‘objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject’ and requires ‘no workable, less intrusive alternatives’ to be present (paras 98-99). In the case at hand, the Court argues that the provision of personalized content and the consistent and seamless use of Meta’s own services do not appear to be necessary for offering a social network service (paras 101-104).

With regard to the legitimate interests of the data controller as a legal basis for data processing, the Court finds that the interests and fundamental rights of users override the interests of a social network provider in offering personalized advertising because users cannot reasonably expect such use of their personal data – even though such social network services are offered free of charge (paras 117-118). Similarly, the Court notes that it is doubtful that the controller’s interest in improving a product or service to make it more efficient or attractive outweigh the interests and fundamental rights of users (paras 122-123). The Court continues by stating that the sharing of information with law enforcement agencies cannot constitute a legitimate interest because it is unrelated to the economic and commercial activity of Meta. At most, such data processing may be justified when objectively necessary for compliance with a legal obligation (para. 124).

In the context of the legal basis involving compliance with a legal obligation, Meta also referred to the need to ‘respond to a legitimate request for certain data’. And in order to claim that the data processing is necessary for the performance of a task carried out in the public interest, it relied on its purpose to ‘research for social good’ and to ‘promote safety, integrity and security’ (para. 129). While the Court left it to the Düsseldorf Court to assess whether Meta is indeed under a legal obligation to collect personal data in a preventive
manner in order to be able to respond to requests from national authorities to provide user data (para. 132), it is in its view unlikely that Meta was entrusted with a task carried out in the public interest to conduct research for the social good and promote safety, integrity and security, given the economic and commercial nature of the data processing (para. 133).

Finally, Meta tried to justify its data processing on the ground that it is necessary to protect the vital interests of data subjects. In response to this claim, the Court stated that Meta, who is pursuing activities of an economic and commercial nature, ‘cannot rely on the protection of an interest which is essential for the life of its users in order to justify, absolutely and in a purely abstract and preventive manner, the lawfulness of data processing’ (para. 137).

Considering these strong statements of the Court, the Düsseldorf Court has little room to still find that Meta’s data processing is consistent with the GDPR. This part of the judgment, in which the Court comments on all legal bases for data processing under the GDPR, will probably be referenced the most in the future considering the clear and outspoken explanations. The Norwegian Data Protection Authority already relied on this part of the judgment to impose a temporary ban on Meta on 14 July 2023 to carry out behavioural advertising based on the surveillance and profiling of users in Norway. It is worth noting that the dominance of Meta did colour the Court’s assessment of the different legal bases. In several instances, the Court refers to the scale of the data processing and its significant impact on users. It therefore seems the judgment supports a more asymmetric interpretation of the duties of data controllers under the GDPR, where a larger scale and impact implies that data controllers are more restricted in their data processing activities.

**Coordination framework set up by the Court**

Another insightful part of the judgment is where the Court sets out a general framework for cooperation between data protection and competition authorities in absence of any specific rules in EU law. Building upon the duty of sincere cooperation of Article 4(3) of the Treaty on the European Union, the Court explains that competition authorities are required ‘to consult and cooperate sincerely’ with data protection authorities to ensure that the
rules and objectives of the GDPR ‘are complied with while their effectiveness is safeguarded’ (paras 53-54). The Court then lays down a number of steps to be followed.

If the conduct at stake or similar conduct has already been the subject of a decision by a data protection authority or the Court, the competition authority cannot depart from the decision (para. 56). Where a competition authority has doubts about how its investigation relates to earlier or ongoing work in the area of data protection, it has to consult and seek the cooperation of the competent or lead data protection authority (para. 57). In turn, the data protection authority must respond to such a request for information or cooperation within a reasonable period of time (para. 58). If the data protection authority does not reply within a reasonable time, the competition authority may continue its investigation. The same applies if the data protection authority has no objection to a competition investigation being continued (para. 59). In the case at hand, the Court concludes that the Bundeskartellamt appears to have fulfilled its obligations of sincere cooperation because it notified the relevant German data protection authorities and the Irish Data Protection Commission as the lead data protection authority who all raised no objections to its actions (para. 60).

As such, the Court leaves it to data protection authorities to control whether a competition authority can check compliance with data protection rules for the purposes of establishing a competition violation. The Court does not prescribe the exact contours of cooperation and thereby invites competition and data protection authorities to come up with more detailed frameworks or protocols to ensure consistency in the application and interpretation of the GDPR. This is now even more relevant with the entry into force of the DMA, which regulates practices to which the GDPR also applies, including personal data combination and data portability. The enforcement of the DMA is in the hands of the European Commission with only an advisory role foreseen for the European Data Protection Supervisor and the European Data Protection Board in the high-level group for the Digital Markets Act. So the roles are reversed in the DMA with the European Commission controlling enforcement, including the application of any relevant data protection concepts.
From the perspective of interpreting data protection concepts for the purpose of establishing a competition violation, the Court also states that a competition authority ‘remains free to draw its own conclusions from the point of view of the application of competition law’ even when a relevant decision on the conduct has already been taken by a data protection authority or the Court (para. 56). This raises the question what room for deviation there is, considering that competition law has its own, autonomous interpretations of various concepts (think of ‘undertaking’ or ‘agreement’ for instance). The judgment seems to leave leeway for competition authorities to set different thresholds for intervention than the GDPR when interpreting data protection rules for the purpose of establishing a competition violation. An example could be a competition authority finding an abuse of dominance consisting of unfair processing of personal data, even though the data protection authority did not establish a violation of the GDPR for the same behaviour.

Outlook

The strong language used by the Court indicates that it regards the *Meta Platforms* case as a clear example of a competition authority legitimately intervening after coordinating with the relevant data protection authorities against behaviour that almost with a doubt violates the GDPR. There will likely be other cases at the intersection of data protection and competition law in the future that are less straightforward. So while the Court opens the door for establishing further synergies between the two legal domains, it also leaves competition and data protection authorities with an assignment to coordinate their respective competences and interpretations of the law.