Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)30

Unclassified

English - Or. English

6 June 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

The intersection between competition and data privacy – Note by the European Union

13 June 2024

This document reproduces a written contribution from the European Union submitted for Item 8 of the 143rd OECD Competition Committee meeting on 12-14 June 2024.

More documents related to this discussion can be found at www.oecd.org/competition/intersection-between-competition-and-data-privacy.htm

Antonio CAPOBIANCO
Antonio.Capobianco@oecd.org, +(33-1) 45 24 98 08

JT03545453

European Union

1. Introduction

1. The European Commission ("Commission") agrees with the findings of the OECD background note that, in the digital economy, the collection, access and sharing of large amounts of data raises issues both under competition and data protection laws. More specifically, practices of data collection and/or data processing are analysed in terms of compliance with data protection rules and respect of the right to privacy, but at the same time such practices may also raise concerns of anticompetitive conduct, leading to or based on the market power stemming from the accumulation of data.

2. Accordingly, there is an increasing intersection and interplay between those rules, and between the authorities enforcing them respectively. As noted by the background note, the relationship is one of complementarity, but also of potential inconsistencies or tensions in enforcement.

3. While competition law and data protection and the authorities enforcing those rules pursue different objectives and perform different functions,[1] both have a crucial role to play in ensuring that undertakings collect and use data in ways that benefit citizens. Those rules protect different, but complementary interests. Accordingly, competition and data protection rules should be used in a complementary way, to ensure consistent outcomes and avoid potential conflicts.

4. In this submission, the Commission will outline the articulation of the relationship of competition and data protection in the European Union ("EU"), based on its case experience (in mergers and antitrust) and the case law of the Union courts. This submission will focus on how data protection considerations may play a role in a competition case, as regards the theory of harm, remedy design and possible objective justifications (Section 2). It will then focus on procedural aspects of cooperation between competition and data protection authorities (Section 3).[2]

2. Data protection considerations in a competition case

5. While issues relating to personal data "are not, as such, a matter for competition law",[3] and violations of the data protection rules are assessed primarily by the competent data protection authorities, data protection considerations can be and have been analysed by the European Commission in competition cases.

6. This can occur when data protection and/or privacy is a relevant parameter of competition in a given market. In this respect, data protection may be considered as a form

[1] Judgment in Case C-252/21 Meta Platforms and Others (General terms of use of a social network), EU:C:2023:537, paragraph 43.

[2] This submission does not discuss other situations where data protection issues may arise in a competition case, such as the handling of personal data and compliance with data protection rules in the context of investigative measures by a competition authority.

[3] Judgment in Case C-238/05 Asnef-Equifax, para. 63, ECLI:EU:C:2006:734.

of quality (or choice) of goods or services.[4] This approach is consistent with the broad interpretation of the notion of "consumer welfare" recognized by the Union courts.[5]

7. Accordingly, the Commission can assess whether a concentration between undertakings or a conduct by a dominant undertaking may affect the level of or choice of data protection offerings, when data protection is an important parameter of competition. Moreover, the ECJ has confirmed that a competition authority can assess compliance with data protection rules, in order to establish whether a conduct amounts to an abuse of dominance.[6] Finally, data protection considerations may also arise in the context of remedies design or objective justifications.

8. The next sections will outline the Commission's considerations on data protection and competition in relation to (i) mergers; (ii) antitrust; and (iii) remedy design and objective justifications, based on its case experience and the case law of the Union courts.

2.1. Merger control

9. In the context of merger control, data protection rules may be relevant when they relate to the competitive process in two main ways: i) existing regulation as limitations preventing data-related effects; and ii) data privacy settings as a non-price parameter of competition.

10. In respect to the former, the Commission may examine if there are certain limitations based on data protection rules preventing data-related effects, both in horizontal (data combination) and vertical (data as input) contexts – e.g. privacy may prevent specific datasets from becoming traded[7]. To the extent the Commission finds that the applicable data protection laws do not prevent data-related effects, the Commission assesses competitive effects as a result of such data combination or data as input contexts. Even if the opposite is true – i.e. existing data protection rules should have a deterrent effect – it cannot be taken for granted that such rules could not be circumvented. In addition, there could also be potential opt-outs or exemptions that could be taken advantage of in the relevant regulation which would need to be considered. Therefore, the Commission has considered whether data protection rules would prevent data-related effects, but has also carried out an "even if" worst-case-scenario assessment, e.g. assessing whether, even if

[4] See Commission Notice on the definition of the relevant market for the purposes of Union competition law, OJ C, C/2024/1645, 22.2.2024, paragraph 15, indicating that "when defining the relevant market, the Commission takes into account the various parameters of competition that customers consider relevant in the area and period assessed" and that "quality should be intended in its various aspects, such as sustainability, resource efficiency, durability, the value and variety of uses offered by the product, the possibility to integrate the product with other products, the image conveyed or the security and privacy protection afforded" (emphasis added).

[5] Under the case law of the Union courts, "harm to consumers" may manifest itself not only in terms of higher prices, but also as reduction of innovation, limitation of choice or deterioration in the quality of goods and services. In this respect, a reduction in the level of data protection or of the options for data protection offered by competitors, as a consequence of the dominant undertaking's conduct, could be seen as harm to consumers in terms of quality or choice.

[6] Judgment in Case C-252/21 Meta Platforms and Others (General terms of use of a social network), EU:C:2023:537, paragraph 47, see section 2.2 below.

[7] Commission decision of 6 September 2018 in case M.8788, Apple/Shazam, paragraphs 225-235; Google/Fitbit, paragraphs 403- 413.

under GDPR[8] it was permitted to combine the data sets of the merging parties, there would be any negative impact on competition. Recent examples of cases where this was done are *Google/Fitbit* and *Meta (formerly Facebook)/Kustomer,* both described below.

11. As per the latter way in which data protection rules may be relevant when they relate to the competitive process, privacy may be an important element of competition on the quality of a products/services. In such circumstances, as with other non-price factors, the Commission assesses whether the merging parties are competing on this parameter and whether the transaction results in a loss of competition in this respect. In other words, pre-merger the two companies were competing with each other on the basis of the data they controlled (or for example privacy settings they had for the relevant data) and this competition would be eliminated by the transaction. This approach was notably adopted in the following cases described below: in Microsoft/LinkedIn,[9] Apple/Shazam,[10] Google/Fitbit,[11] and Meta (formerly Facebook)/Kustomer.[12]

12. In Microsoft/LinkedIn, the Commission found that privacy was an important parameter of competition for users of professional social networks,[13] and that post-merger Microsoft would have the ability and incentive to foreclose competitors of LinkedIn, including professional social networks that offered more privacy-friendly options, valued by consumers. The transaction was cleared following commitments by Microsoft that ensured that other professional social networks would not be foreclosed on Microsoft's operating system and applications.

13. In Apple/Shazam, the Commission's in-depth investigation focused on whether Apple would obtain access to commercially sensitive data about customers of its competitors for the provision of music streaming services in the EEA (i.e. user behavioural data, which was not licensed by Shazam to third parties), and whether such data could allow Apple to directly target its competitors' customers and encourage them to switch to Apple Music, resulting in a competitive disadvantage vis-à-vis competitors not having access to such data. The Commission found that the integration of Shazam's and Apple's datasets on user data would not confer a unique advantage to the merged entity in the markets on which it operates. Shazam's data was found to not be unique, and Apple's competitors would still have the opportunity to access and use similar databases. However, the Commission noted that its findings in a merger decision do not release companies from respecting all relevant data protection laws.[14]

14. In *Google/Fitbit*, the Commission comprehensively investigated data and privacy implications, to the extent that they could translate into competition concerns. In particular, the Commission examined the data collected via Fitbit's wearable devices and did not find evidence that privacy was a parameter of competition in wearables in the EEA (as it did

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[9] Commission decision of 6 December 2016 in case M.8124, Microsoft/LinkedIn.

[10] Commission decision of 6 September 2018 in case M.8788, Apple/Shazam.

[11] Commission decision of 17 December 2020 in case M.9660, Google/Fitbit.

[12] Commission decision of 27 January 2022 in case M.10262, Meta (formerly Facebook)/Kustomer.

[13] Microsoft/LinkedIn, paragraph 350.

[14] Apple/Shazam, paragraph 226, footnote 251.

instead in the *Microsoft/LinkedIn* case described above). However, the Commission found that by acquiring Fitbit, Google would acquire (*inter alia*) the database maintained by Fitbit about its users' health and fitness. By increasing the already vast amount of data that Google could use for the personalisation of ads, the transaction would therefore raise barriers to entry and expansion for Google's competitors for these services to the detriment of advertisers, Eventually, Google committed to maintain a technical separation of the relevant Fitbit user data. The data will be stored in a "data silo" which will be separate from any other Google data that is used for advertising.

15. In *Meta (formerly Facebook)/Kustomer*, the Commission investigated what data Meta would obtain from Kustomer's customers and if it would obtain a competitive advantage as a result. Kustomer offers a business-to-business product and does not own the data of its business customers. Access to data would be dependent on agreements with its business customers who need consent from their end customers. The Commission found that because of Kustomer's small size, even taking into account its potential growth, the amount of additional data will not be significant. Moreover, rival providers of online display advertising services have, and will continue to have, access to similar commercial data because of the strong commercial interest of businesses in sharing such data with both Meta and rival advertising platforms in order to measure and optimise the performance of their ad campaigns. Therefore, the Commission concluded that any additional data that Meta may gain access to for the purposes of improving its online display advertising service would not result in a significant negative impact on competition between providers of online display advertising services.

16. To conclude, data protection rules and the non-tradability of data may be circumvented through external growth strategies (i.e. concentration that allows accumulation of non-tradable data, as long as availability of such data is relevant for competition). This led to data considerations arising in several cases in recent years. For example, the access to data, the role of data as a barrier to entry and expansion and whether a transaction leads to an accumulation of data to the detriment of competition and consumers are already today considered in the Commission's merger reviews. Therefore, the regulatory framework of EU merger control is sufficiently flexible to also tackle the specific implications of data-related effects in the Commission's merger reviews.

2.2. Antitrust

17. As mentioned above, data protection considerations may be a relevant parameter of competition. Therefore, in principle a conduct by a dominant undertaking affecting the level, choice or quality of data protection available to consumers could amount to an abuse of dominant position under Article 102 TFEU. In this respect, a distinction can be made between abuses where data protection considerations are part of the effects stemming from a conduct and abuses where those considerations are part of the conduct itself.

18. The former scenario would concern the assessment of an exclusionary conduct (unrelated to data protection), that potentially affects competitors offering a higher level of data protection than the dominant undertaking, in a market where data protection is valued by consumers. In this situation, the fact that the conduct affects data protection can be factored in the analysis of the exclusionary effects of an abuse, under the broad notion of harm to consumers.[15]

[15] See paragraph 6 above.

19. The latter scenario would concern a conduct which has as its object data gathering and the level/quality/type of data protection itself. The OECD background note explains that such conducts can include behaviours of data privacy degradation or excessive data collection, which: (i) could be assessed as exploitative abuses, in the form of excessive pricing or unfair trading conditions; and (ii) could also have an exclusionary dimension, if by collecting data from users, the dominant undertaking raises barriers to entry and protects its market position.[16] In both instances, the Commission considers that the main challenge for running these cases would be how to assess and measure whether the level of data protection is degraded and whether the data gathering is excessive, as a relevant benchmark needs to be established.

20. In this respect, as mentioned by the OECD background note, qualitative benchmarks could be used, such as the relevant data protection rules.[17] This approach has been confirmed in the *Meta* judgment, where the ECJ established that when assessing whether a dominant undertaking's conduct amounts to an abuse of dominance, "*the compliance or non-compliance of that conduct with the provisions of the [General Data Protection Regulation] may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers*".[18]

21. Accordingly, the Commission agrees that a competition authority can evaluate compliance with the data protection rules as part of the assessment of whether a dominant undertaking's conduct amounts to an abuse of dominance. However, such analysis of compliance with data protection rules would not be in itself sufficient to establish an abuse of dominance, but only a part of the competitive assessment. It would be necessary to also establish the other elements of an exclusionary or exploitative abuse to the requisite legal standard (e.g., exclusionary effects in the case of an exclusionary abuse).

22. Moreover, in light of the complementarity between the competition and data protection rules, any assessment by a competition authority of data protection rules is only for the purpose of the competitive assessment: it does not replace the compliance assessment by the competent data protection authorities.[19]

---

[16] Background Note, paragraphs 45 – 49.

[17] A similar approach would be to carry out an assessment under Article 102(a) TFEU, based on the case law of the European Court of Justice on exploitative abuses. This would require an assessment of the "fairness" of the trading conditions of a dominant undertaking collecting data, by using the principles of necessity, proportionality and transparency as relevant benchmarks. The Commission further notes that an assessment of these conducts could, in principle, also be carried out in purely quantitative terms (e.g., by measuring the amount of data collected). However, it would be particularly difficult in practice to assess a non-quantitative element, such as the level and value of data protection, as a form of quality for consumers, without reference to a clear legal benchmark.

[18] Judgment in Case C-252/21 Meta Platforms and Others (General terms of use of a social network), EU:C:2023:537, paragraph 47. See also paragraph 43, where the ECJ noted that "there is no provision in [the GDPR] that prevents the national competition authorities from finding, in the performance of their duties, that a data processing operation carried out by an undertaking in a dominant position and liable to constitute an abuse of that position does not comply with that regulation". With the caveat mentioned in point 22 below.

[19] Ibid., paragraph 49.

23. Finally, carrying out such analysis also has procedural implications, as the ECJ established in the *Meta* judgment that there should be cooperation and coordination with data protection authorities.[20]

2.3. Remedy design and objective justifications

24. The Commission notes that data protection considerations may also arise in the context of remedies design, in particular in abuse cases concerning data-related conducts but also in merger control procedures.

25. For instance, in a refusal to supply case, where the input to which access is refused is data of the dominant undertaking, the most straightforward remedy would consist of mandating data access. However, such remedy could likely raise issues of data protection, in particular if the data are stake include personal data gathered by the dominant undertaking. Before further sharing the data, a dominant undertaking would need to inform its users that their data have to be made available to a third party for the purpose of compliance with an antitrust remedy and seek their specific and explicit consent. While this approach would seem straightforward in theory, it may be difficult to implement in practice.[21] Similar considerations may arise in the context of a remedy ensuring data portability for users, although in those scenarios, users are entitled to choose to port their data themselves.

26. Where the Commission identifies a data-related concerns in merger control, the possible solutions that could be explored depend on the pre-transaction situation (e.g. whether the data was traded or non-traded) and the type of data involved.

27. In *Google/Fitbit*, a merger that increased the merged entity's data advantage to such an extent that it was found to impede rivals' ability to compete against the services provided by Google, a commitment not to use the acquired data related to the services/markets where concerns arose (a so-called "data silo") was found suitable to solve the competition problem in light of the very specific facts of the case. Notably, the case involved sensitive health data which, by nature, could not lend itself to an access commitment. As a result, the Commission considered that a data-related issue in a situation where such data could not be made available to competitors could be resolved by maintaining the relevant data in a separate silo. In this particular case, such separation was technically possible, and the length of the commitment (10 years) was sufficient, yet flexible enough for possible future market

[20] See section 3 below.

[21] See in that regard, the Report of the Special Advisers to Commissioner Vestager "Competition policy for the digital era", available at https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf (the "Special Advisers' Report"), p. 80: "In some settings, obtaining valid consent for uses that do not immediately benefit the data subject granting consent may be burdensome". In this respect, data anonymization could solve the issue of consent, as the General Data Protection Regulation does not apply to anonymised data. This is the approach adopted by certain EU regulations, for instance Article 6(11) of the Digital Markets Act, pursuant to which a gatekeeper for search engines must provide to third party providers of online search engines access to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines, subject to anonymization of those data. However, this possible solution can also present challenges. In particular, anonymization could be technically complex. Moreover, anonymization might still entail certain privacy risks, see See Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques (WP216)' (2014) 9, pp. 3-4, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, and Special Advisers' Report, p. 86.

changes to be taken into account (given that some future data uses may not exist at the time of the decision). Given the particular circumstances of the case and its precise theory of harm, the suitability of similar commitments to other situations is unclear. Evidently, market participants' input on remedy proposals are key to understanding whether the above factors exist in each particular case. A positive market test of the remedies would need to fully support the design and effectiveness of the remedy proposed.

28. Furthermore, in theory, a dominant undertaking might also raise data protection considerations as a form of objective justification, for instance by arguing that its conduct benefits consumers by ensuring a higher degree of data protection. Any such arguments would likely have to be assessed under the general framework for objective justifications developed in the case law of the Union courts.[22]

3. Procedural issues

29. As mentioned above, the fact that a competition authority may assess data protection considerations and the relevant rules in the context of a competition case also has procedural implications. In particular, a competition authority must coordinate its investigation and assessment with the competent data protection authorities.

30. Specifically, in the *Meta* judgment, the ECJ noted that "*when national competition authorities are called upon, in the exercise of their powers, to examine whether an undertaking's conduct is consistent with the provisions of the GDPR, they are required to consult and cooperate sincerely with the national supervisory authorities concerned or with the lead supervisory authority, all of which are then bound, in that context, to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded*".[23]

[22] An objective justification may consist in an objective necessity or efficiencies. An objective necessity must be based on evidence that a dominant undertaking's behaviour was objectively necessary to achieve a certain aim, which can include considerations of public health, safety or other public interest considerations. However, the Union courts have specified that a dominant undertaking cannot remove products it considers inferior or dangerous, or to ensure compliance of other undertakings with the law, see judgment of 12 December 1991, Hilti v Commission, T-30/89, EU:T:1991:70, paragraphs 116-118. Furthermore, an objective necessity defence will be accepted only if the actual or potential exclusionary effects resulting from the conduct are proportionate to the alleged necessary aim, see judgment of 12 May 2022, Servizio Elettrico Nazionale and Others, C-377/20, EU:C:2022:379, paragraph 103. As regards efficiencies, a dominant undertaking escapes the prohibition of Article 102 TFEU if it proves that the exclusionary effects resulting from its conduct are counterbalanced, or even outweighed, by advantages in efficiency that also benefit consumers, see judgment of 6 October 2015, Post Danmark, C-23/14, EU:C:2015:651, paragraph 48, and judgment of 6 September 2017, Intel v Commission, C-413/14 P, EU:C:2017:632, paragraph 140. Four cumulative conditions must be met for an efficiency defence to succeed: (i) the efficiencies likely resulting from the conduct counteract any likely negative effects on competition and the interests of consumers; (ii) those gains have been, or are likely to be, brought about as a result of this conduct; (iii) the conduct is necessary for the achievement of those efficiency gains; and (iv) the conduct does not eliminate effective competition, by removing all or most existing sources of actual or potential competition. See judgment of 27 March 2012, Post Danmark, C-209/10, EU:C:2012:172, paragraph 42.

[23] Judgment in Case C-252/21 Meta Platforms and Others (General terms of use of a social network), EU:C:2023:537, paragraph 54.

31. Accordingly, the ECJ explained that if the conduct by a dominant undertaking related to data protection issues has already been assessed by a competent data protection authority, the competition authority "cannot depart" from that authority's decision, although *"it remains free to draw its own conclusions from the point of view of the application of competition law*"; if, on the other hand, that competition authority has doubts on the decision of data protection authority, or the conduct of the dominant undertaking is being simultaneously investigated by a data protection and a competition authority, or it is only the competition authority that is investigating, then that competition authority "*must consult and seek their [of the data protection authorities] cooperation in order to dispel its doubts or to determine whether it must wait for the supervisory authority concerned to take a decision before starting its own assessment*".[24]

32. The Commission notes that the approach articulated by the ECJ in the *Meta* judgment is aimed at ensuring coordination and consistent outcomes between different and complementary regulatory instruments, and at avoiding duplication of procedures and possible penalties. This is also consistent with the *Bpost* judgment, concerning *ne bis in idem*.[25]

33. The Commission notes that it does indeed seek cooperation with the competent data protection authorities, to ensure consistent outcomes and knowledge sharing. This has been the case particularly in merger cases touching upon data issues. For instance, in the *Google/Fitbit* case, the Commission worked in close cooperation with the European Data Protection Board ("EDPB") and the European Data Protection Board Supervisor ("EDPS", which provides the EDPB's secretariat), to understand the regulatory framework applicable to personal data processing by Google and Fitbit. The EDPB also provided feedback, on behalf of its members, to the market investigation and to the remedies' market testing.

4. Conclusion

34. The Commission agrees that there is a growing intersection and interaction between competition law and data protection rules. These instruments pursue different, but complementary objectives.

35. The relation between competition and data protection concerns both issues of substance and procedure. As regards the former, considerations on data protection may be factored in the competitive assessment, as data protection and privacy may be a relevant parameter of competition. As regards the latter, the respective authorities may have to (or are in fact required) to coordinate and cooperate, to ensure consistent outcomes of enforcement.

36. The Commission has, to date, factored data protection considerations into competition cases, in particular in the assessment of mergers where privacy was a relevant parameter of competition. As confirmed by the *Meta* judgment, compliance with data protection rules can be a relevant factor for the assessment of conduct in a competition case. However, this assessment is distinct from the assessment of the competent data protection authorities. The *Meta* judgment has also emphasised the importance of cooperation and coordination between competition and data protection authorities.

[24] Ibid., paragraphs 56 – 57-

[25] Judgment of 22 March 2022, Bpost, C-117/20, EU:C:2022:202.