Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)45

Unclassified

English - Or. English

17 May 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

The intersection between competition and data privacy – Note by Austria

13 June 2024

This document reproduces a written contribution from Austria 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

JT03543915

Austria

1. Introduction

1. In Austria, the synergy between competition law and data privacy law is particularly pronounced, reflecting a broader, global trend to address the unique challenges posed by the digital economy. This convergence is driven by the common goal of protecting consumers and market participants alike. It aims to foster an environment where consumer welfare and privacy standards are not mutually exclusive but are seen as complementary pillars supporting a fair and dynamic market landscape. In this context, cooperation between national regulatory authorities is becoming increasingly important. The impetus for this increased focus on cooperation also stems from recent jurisprudance at the European level, which highlights the complex interplay between ensuring competitive markets and protecting personal data in the digital age. This evolving situation presents both opportunities and challenges that require a nuanced approach.

2. The relationship between Competition and Data Privacy Law in Austria

2.1. The evermore interaction between Competition and Data Privacy Law

2. Both antitrust law and data protection law represent important instruments to create a level playing field in an increasingly data-driven economy in which companies can operate and individuals are protected accordingly.

3. At first sight, antitrust law and data protection/privacy law seem to pursue quite different objectives. The aim of effective antitrust law is to protect an efficient market in which consumer welfare is increased by appropriate competition in the relevant market. Data protection law, on the other hand, seeks to protect constitutionally guaranteed interests in confidentiality and privacy. The differences lie primarily in the broader, economic oriented approach of antitrust law as opposed to the protection of individual, personal rights in data protection.

4. A closer look, however, reveals that the core of both legal regimes is an abstract attempt to prevent the exploitation of imbalances, ultimately to the benefit of consumers (data protection law) or other disadvantaged market participants (antitrust law). As rightly noted in the relevant literature, both legal systems seek to strengthen consumer confidence in digital markets and preserve consumer choice.

5. Another important intersection between antitrust law and data protection is in the area of data portability. The free transferability/ movability of data is one of the most important factors in promoting competition in an increasingly data-based economy. The relevant regulations within the competition and privacy policy rules allow individuals to transfer certain (personal) data between different providers and impose obligations on those providers to do so. Such data portability rules can facilitate market entry, break the market power of certain companies and promote competition overall. However, the signs clearly point to increased competition.

6. In addition to this data-driven competition, data protection can also be seen as an element of a product or service offered. This is where the interaction between data protection law and antitrust law becomes particularly evident. One might think, for example, of the change in WhatsApp's terms of use and privacy policy in 2021, which - at

least temporarily - led to an increased switch to other messaging services with higher data protection standards. Data protection can thus be a quality feature of a product or service that companies can use to differentiate themselves and thus promote competition. This theory, referred to as "privacy-as-quality", is increasingly being considered in the competition assessment, especially in the area of merger control and abuse cases. It is expected that this type of "privacy led competition" will play an increasingly important role in the future.

7. Despite the aforementioned complementarity or partial parallelism, it is important to keep in mind that antitrust and data protection law remain areas of law. As antitrust rules are much broader formulated than those of data protection law, it seems comparatively easier for competition authorities to incorporate data protection assessments into competition assessments. However, the question of how to deal with infringements of the GDPR that appear to give a company an unjustified competitive advantage remains largely unresolved, apart from the Meta case.

8. Against the background of an increasingly strong interaction between data protection and antitrust law, a brief insight into the specific Austrian legal and the practice of the AFCA regarding dawn raids in the context of data protection will be presented below.

2.2. The legal framework and relationship of the Austrian competition law and the Federal Act concerning the Protection of Personal Data

9. Section 1 of the Austrian Data Protection Act (DPA) contains a fundamental right to data protection. According to Section 1 (1) DPA, "everyone" has the right to secrecy of personal data concerning him or her, in particular with regard to the protection of his or her private and family life, provided that there is a legitimate interest. In addition, Section 1 (3) of the Data Protection Act provides for a right of access, rectification and deletion for everyone. The peculiarity of this regulation lies in the fact that not only natural persons are protected by Section 1 DPA, but also legal persons who are not protected by the GDPR.

10. In the past, the legislator has tried several times to replace "everyone" with "natural persons", but has not been able to obtain the necessary majority in Parliament, since this provision is a constitutional provision, the amendment of which requires an increased majority in Parliament.

11. Therefore, under Austrian law, a company also has the possibility to lodge a data protection complaint with the Austrian Data Protection Authority if it feels that its right to secrecy has been violated. This may be the case, for example, if internal company documents are disclosed to third parties.

12. In practice, however, Section 1 DPA has no significant impact on competition law: In the case of merger notifications, the notifying parties themselves disclose internal company data and documents to the AFCA, or an exchange with e.g. competition authorities in other countries or the European Commission takes place with the consent of the parties by way of a waiver. Theoretically, it would be possible to file a complaint in the event of a dawn raid (see also point 2.3).

13. As a public authority, the AFCA requires a legal basis for the processing of personal data according to Section 1 (2) DPA, if no consent is given. It is obvious that the company that is the target of a dawn raid does not give its consent, which means that the existence of a legal basis is necessary for lawfulness (cf. Article 18 of the Austrian Constitution).

14. Pursuant to Section 11(3) of the Competition Act, the AFCA is authorised to process all personal data necessary to achieve its objectives pursuant to Section 1(1) and to fulfil its tasks pursuant to Section 2(1) and (2).

15. It should also be noted that pursuant to Section 11 (4) Competition Act, the right of access under Art. 15 GDPR may not be exercised if it would contradict the objectives of the AFCA or impair the fulfilment of the tasks assigned to the AFCA. The right of access pursuant to Art. 15 GDPR is therefore de facto not applicable. In practice, this provision does not apply anyway, as the AFCA generally investigates legal entities and not natural persons.

16. In September 2023, the Austrian Federal Administrative Court, as the court of first instance of the Austrian Data Protection Authority, ruled that a legal person could not base its complaint on Section 1(1) and (3) of the Data Protection Act and therefore did not have the right to lodge a complaint. The reasons given were that a constitutional interpretation of the provision on the right to lodge a complaint with the Austrian Data Protection Authority in the sense of an extension contrary to the content of the standard and the express wording of Section 4(1) of the DPA, according to which the statutory part of the DPA also actively entitles a legal person to lodge a complaint, is out of the question because the wording of the provision is unambiguous. With regard to the drafting of Section 24 of the DPA, the legislator did not fail to identify an unintentional loophole, as Section 4(1) of the DPA expressly adopts the provisions on the scope of the GDPR as implementing provisions. As a result, a legal entity does not have the possibility to lodge a complaint on the basis of Section 1 of the Data Protection Act in conjunction with Section 24 of the Data Protection Act.

17. The Austrian Data Protection Authority has lodged an official appeal against this judgement. The case is still pending before the Austrian Supreme Administrative Court. It remains to be seen whether the Austrian Supreme Administrative Court will follow the opinion of the Austrian Federal Administrative Court.

2.3. Data protection and dawn raids - the approach by the AFCA

18. The peculiarities of the Austrian data protection law described above, as well as the exceptions or limitations thereof for investigations by the AFCA, have a decisive impact on the conduct of dawn raids. Such inspections represent a particularly intensive encroachment on the fundamental rights of the data subject and therefore always require a proportionate approach. Of particular importance for the present article are the right to privacy (Art. 8 ECHR; Art. 7 CFR) and the right to data protection (Art. 8 ECHR; Section 1 DPA). These rights are to be respected as far as possible when conducting a raid.

19. The right to data protection is based on the right to privacy, and distinguishes between personal and non-personal data. The GDPR also focuses exclusively on personal data. As long as such data are concerned, the scope of the fundamental right to data protection is open. In Austria, the national constitutional provision of Section 1 DPA must also be taken into account. As mentioned above, Section 1 DPA provides even more comprehensive protection than the ECHR and the GDPR, as it applies to legal persons and (under certain circumstances) also protects particularly sensitive economic data.

20. The right to data protection regularly applies in the context of dawn raids carried out by the AFCA. During dawn raids, the AFCA searches in particular for antitrust relevant communications, which by their nature involve a certain degree of personal connection, i.e. personal data. As both the collection and processing of data fall within the scope of protection, the right to data protection is generally applicable during the investigation and collection of data. In order to minimise these intrusions and to make them as transparent as possible for the data subject, the AFCA has adopted the following practical approach:

21. The dawn raid is based on a judicial warrant. In particular, electronic data (such as server drives, email accounts, storage devices, etc.) will be secured and analysed at the

AFCA premises after the dawn raid. Due to technical limitations, it cannot be excluded that private, confidential data of the respective (natural) targets/persons will be secured. Such a comprehensive data backup is permissible, especially if the sorting out of non-case relevant (often private) data on site would be disproportionately burdensome. Given the sheer volume of data that needs to be backed up these days, this is often the case. In order to minimise disruption to the business, companies themselves usually have an interest in a speedy solution.

22. The relevant data is backed up on site by means of an image or logical copy, usually directly from the server. Representatives of the company or its lawyers will have the opportunity to be present throughout the inspection and will be provided with a detailed protocol at the end of the inspection outlining what electronic data has been secured. The company is also given the opportunity to make a copy of the secured data.

23. As a security measure, the hard drives are then packaged in numbered sealed bags and stored in a safe during transport to the AFCA, which is accessible only to designated staff. The evaluation of the secured data takes place in a dedicated "evaluation room" where the computers are not connected to the Internet. The access area to the evaluation room is under constant video surveillance and only the relevant case handlers and the IT forensic team have access to the secured data.

24. After evaluating the data, the AFCA will decide which data or documents will be included in the investigation file. Only this data can potentially be used in further proceedings. Once again, the company concerned will be informed and given the opportunity to make a copy of the data to be included in the file. This transparent approach ensures that the company concerned can follow exactly what data is being processed by the AFCA at all stages of the procedure.

25. Upon the final conclusion of the proceedings, the electronic data will be irreversibly erased from all storage media. Through this procedure, the AFCA has largely managed to avoid data protection concerns of the data subjects.

3. The cooperation between the competent authorities in Austria

26. In principle, Art. 22 of the Austrian Constitution enables all federal bodies to provide mutual assistance within the scope of their statutory activities. This means that the authorities may or must provide mutual assistance in order to fulfil their tasks.

27. Advancing digitalisation and its regulation require the AFCA and the Austrian Data Protection Authority to cooperate more closely with other supervisory and regulatory authorities in Austria, but also among themselves, in order to ensure the most consistent approach possible. This cooperation has already begun and will be intensified in the future. It is important that each authority acts within the scope of its competence.

28. The mutual exchange between national competition and data protection authorities should be intensified, in particular following the judgement of the European Court of Justice in Case C-252/21. The effects of this judgement in Austria are not yet clear. To date, there have been no cases known to the AFCA in Austria in which the outcome of this ruling has had an impact. Due to the increasing importance of data traded as part of a business model, it is only a matter of time before similar situations arise in Austria.

29. Accordingly, increased cooperation between the AFCA and the Austrian Data Protection Authority is essential in the future. Cooperation will not only create legal certainty, especially after the aforementioned judgment, but can also serve to support and learn from each other.

30. However, the reciprocal exchange of information may prove difficult if the results of secret investigations are involved. This widens the circle of those informed and increases the risk of leaks of secret information. There is also the practical question of how one authority can learn about the activities of the other, since both are subject to confidentiality.

31. In addition, cooperation is associated with increased human resources. Nevertheless, it can be assumed that the advantages of cooperation outweigh the disadvantages.

4. Conclusion

32. In conclusion, it is important to underline how closely competition law and data privacy law are linked. Cooperation between regulators is an important step forward in addressing the multiple challenges of the digital environment.

33. The synergy identified herein is not merely a regulatory convergence but a strategic alignment towards safeguarding consumer welfare and privacy as interlinked objectives. This alignment is of paramount importance in fostering a competitive yet fair digital environment where competition thrives without compromising data protection standards.

34. Having said that, it is important to recognise the complementary nature of consumer welfare and consumer privacy.