Organisation for Economic Co-operation and Development

DAF/COMP/M(2024)2/ANN6/FINAL

Unclassified

English - Or. English

1 August 2025

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Cancels & replaces the same document of 3 June 2025

Executive Summary of the Roundtable on The Intersection between Competition and Data Privacy

Annex to the Summary Record of the 143rd Meeting of the Competition Committee

12-14 June 2024

This Executive Summary by the OECD Secretariat contains the key findings from the discussion of the roundtable on The Intersection between Competition and Data Privacy, held during the 143rd meeting of the Competition Committee on 12-14 June 2024.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

Please contact Mr Antonio Capobianco if you have questions about this document.
Email: Antonio.CAPOBIANCO@oecd.org

JT03569791

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Executive Summary of the Roundtable on The Intersection between Competition and Data Privacy

On 13 June 2024, the OECD Competition Committee and the Working Party on Data Governance and Privacy of the OECD Digital Policy Committee held a joint roundtable to explore the links between competition and data privacy. Considering the background note prepared by the OECD Secretariat, the written contributions and the discussion, the following key points emerged:

1. Competition and Data Privacy laws share common features, while significantly differing in terms of scope, goals, conceptual frameworks, and procedures.

Competition law and data privacy laws are two distinct legal regimes with different goals and frameworks. This reflects the different rationales behind their establishment and evolution: while competition law integrates an economic perspective, data privacy laws are mostly based on the concept of privacy as a fundamental right. This original divergence explains why the two regimes have traditionally been considered as separate.

However, competition law and data privacy laws share "family ties", as both pursue an overarching objective of protecting the welfare of the individual, whether as a consumer or as a data subject.

In the context of digital markets in particular, with the emergence of data-driven business models and in instances where the "data subject" or "individual" and the "consumer" clearly overlap, their interactions have become increasingly relevant. This had led to the growing attention around the concomitant application of the two legal regimes.

2. Competition authorities increasingly see privacy as a component of quality, and therefore a key element of non-price competition, and include privacy considerations into their assessments. At the same time, data protection authorities are starting to take market dynamics into account for their analyses.

With the digitalisation of the economy, an integrationist approach has been gaining importance in recent years. The strong link between a firm's dominance, its data processes, and competition in certain markets can support the inclusion of data privacy considerations in competition authorities' assessment, as shown in the *Meta Platforms* case. A number of jurisdictions' interventions also confirmed this trend by emphasising the existing synergy between competition law and data privacy, including in terms of strategic alignment towards interlinked objectives.

This shift has led to the emergence of new theories of harm, built around data and data privacy, such as data privacy degradation, where data privacy is seen as a non-price parameter of competition and the weaker data privacy protection offered to users as a reduction in quality. During the roundtable another example of how data privacy degradation could take place was addressed, which pertains to so-called concealed data practices, i.e. where platforms offer weak privacy protection while hiding the extent of these conditions and data processing from consumers. These practices can have both exploitative and exclusionary effects, similarly to another theory often discussed in the context of digital markets, privacy policy tying.

From the perspective of data protection authorities, so far the attempt to integrate competitive parameters into their analysis has focused on the balance of power between controller and data subjects. Indeed, the notion of imbalance between data subjects and

controller, may provide a basis to consider a firm's market position in the context of privacy and personal data protection enforcement.

3. The interaction between competition and data privacy laws can generate important synergies and complementarities. However, trade-offs and challenges may also arise between the two regimes, undermining their effectiveness.

Both systems aim at protecting the welfare of the individual, whether as a consumer or as a data subject; consequently, the implementation of one can complement and enhance the effectiveness of the other.

For instance, the enforcement of data protection laws can reinforce competition by preventing dominant undertakings from obtaining an unfair competitive advantage through unlawful data collection or processing. Similarly, competitive markets can lead to higher levels of data privacy offered to consumers, especially when companies compete on the quality of the product/service, where data privacy can be seen as an element of quality, and a key non-price parameter of competition.

However, the concomitant application of the two regimes can often lead to challenges, and interventions with potential complementarities can also carry the risk of divergent effects. Indeed, as also highlighted during the roundtable, characterising the relationship between data privacy and antitrust only in terms of synergy and complementarities can be seen as a fallacy.

Two key examples of this pertain to data portability and interoperability requirements.

Further, abuse of dominance cases in recent years have brought to light potential tensions in the antitrust-privacy interplay. This is the case of the so-called data privacy defence, which sees the use of an increased level of data privacy offered to end users as a justification for potentially anticompetitive conducts. Enforcement action thus requires differentiating between cases where the data privacy measure used as a shield is within the limits of what is mandated by data privacy law, and cases where it goes beyond that.

Finally, parallel investigations by data privacy and competition authorities can also result in inconsistent approaches, especially if remedies are considered, for example in instances where questions around interoperability or access to data are at stake. Frameworks for co-operation between authorities can help reduce frictions and divergences.

4. There is an emerging consensus that effective cross-regulatory co-operation, to achieve more integrated enforcement strategies, is paramount in digital markets. A growing number of competition and data protection authorities are joining forces to pursue their mandates in a coordinated way based on a variety of models.

Closer interaction between regulators is indispensable in the context of the digital economy and presents numerous benefits. Firstly, cooperation allows authorities to deepen their knowledge and to ensure consistent outcomes.

Secondly, better cooperation would allow to reinforce the efficiency of the investigation. As explained by during the roundtable, co-operation can facilitate access to mutual expertise, as well as reduce the length of investigations, with coordination of procedures and clarity in terms of competencies. Thirdly, cooperation can further strengthen consumer protection, with a number of jurisdictions starting to integrate data privacy as part of quality criteria in their assessments.

While the need for co-operation is now well-established, the most effective means to do so and the practical implications of such co-operation are still being explored. Jurisdictions worldwide showcase a range of models for co-operation, each offering interesting insights and lessons.

While informal models of cooperation are generally characterised by the absence of legislative reforms or a formal legal basis for the cooperation between the two authorities, formal models rely on legislative provisions allowing a deeper level of cooperation, for example thanks to the sharing of data and information.

Certain agencies have both data privacy protection and competition powers. Having a centralised combination of powers can help ensure the consistency of decisions, may allow for a better understanding of data-related dynamics in digital markets, as well as a more effective inclusion of different policy considerations in enforcement cases, reducing the need for external coordination and the risk of divergences.

Finally, a number of jurisdictions have created new fora for exchange and co-operation to respond to the recent enforcement challenges posed by digital markets and promote coherent approaches to regulation in the digital sphere.