CENTRAL EUROPEAN UNIVERSITY

FROM RIGHTS TO REMEDIES: THE INTERPLAY OF DATA PROTECTION AND COMPETITION LAW IN THE CONTEXT OF DATA PORTABILITY

by Azra Selvi Kapu

Submitted to Central European University
Department of Legal Studies

In partial fulfilment of the requirements for the degree of Master of Global Business Law and Regulation

Supervisor: Prof. Marco Botta
Vienna, Austria
2025

COPYRIGHT NOTICE

For bibliographic and reference purposes this dissertation should be referred to as:

Kapu, Azra Selvi; 2025, "From Rights to Remedies: The Interplay of Data Protection and Competition Law in the Context of Data Portability", LL.M. thesis, Legal Studies, Central European University, Vienna.

AUTHOR'S DECLARATION

I, the undersigned, Azra Selvi Kapu, candidate for the LLM degree in Global Business Law and Regulation declare herewith that the present thesis titled "From Rights to Remedies: The Interplay of Data Protection and Competition Law in the Context of Data Portability" is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography.

I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright.

I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Vienna, 15.06.2025

Azra Selvi Kapu

ABSTRACT

The intersection of data protection and competition law in the enforcement of data portability rights presents fundamental questions about how these rights can be effectively implemented to enhance user autonomy and promote market competition. While Article 20 of the General Data Protection Regulation (GDPR) established a groundbreaking framework for individual data portability rights, its practical effectiveness remains constrained by significant limitations including narrow scope restrictions, technical implementation challenges, and enforcement gaps that particularly affect competitive digital markets.

Subsequent EU legislation, including the Digital Markets Act and Data Act, has expanded data portability obligations beyond the GDPR's framework, reflecting a regulatory evolution from purely user-centric rights toward broader competition-oriented tools. However, these instruments retain limitations in addressing market-wide competitive concerns, particularly regarding enforcement mechanisms and scope of application.

The centerpiece of this analysis is the Turkish Competition Authority's decision in the *Sahibinden* case, which imposed data portability obligations as behavioral remedies under competition law. This landmark decision demonstrates how competition authorities can address data portability restrictions as abuse of dominance, going beyond traditional data protection approaches to mandate comprehensive technical infrastructure for seamless data transfers. The Turkish approach overcame key GDPR limitations by requiring bidirectional data portability, encompassing broader data categories, and ensuring real-time updates without consent-related fragmentation.

The analysis concludes that effective data portability enforcement requires coordination between data protection and competition law frameworks. The *Sahibinden* decision provides a

valuable template for European competition authorities, demonstrating that competition law remedies can be more effective than individual rights-based approaches in achieving systematic market-level changes. Competition enforcement can recognize data portability restrictions as clear abuse of dominance when they raise switching costs and suppress multi-homing, offering a roadmap for addressing contemporary digital market challenges through sophisticated behavioral remedies.

TABLE OF CONTENTS

INTRODUCTION

In the evolving landscape of digital rights and data governance, the concept of user autonomy has gained increasing prominence. One of the key manifestations of this shift is the principle of data portability, a right designed to enhance control over data in digital environments. It enables users to take control over their personal information by facilitating access. In addition, it allows the migration of data from one controller to another. The idea of portability is not entirely new, for instance, as early as 1996 in the United States, telecom providers were required to allow users to keep their phone numbers when switching to a different service provider.[1] One other illustrative example of data portability in practice is Google Takeout, a service that enables users to download the data they have generated within Google's ecosystem. By way of this tool, Google offers its users the possibility to download the data that they have created in Google's social networking site Google+ in a variety of open formats so that users can easily import the data into other internet services.[2]

Data portability enhances individual control over personal data while also serving as a regulatory instrument with broader implications for privacy, consumer rights, and market competition. As digital markets grow, large platforms accumulate vast and diverse user data, giving them a significant competitive edge. This data concentration reinforces platform dominance through lock-in effects and high switching costs. In light of these concerns, policymakers and competition authorities have increasingly recognized data portability not just

[1] 'OECD, *Data Portability, Interoperability and Digital Platform Competition* (OECD Competition Committee Discussion Paper, 2021) https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf accessed 10 June 2025,15.

[2] Inge Graef, Jeroen Verschakelen and Peggy Valcke, 'Putting the Right to Data Portability into a Competition Law Perspective' (Social Science Research Network, 2013) 3 <https://papers.ssrn.com/abstract=2416537> accessed 3 February 2025.

as a user right, but also as a potential tool to promote fair competition and reduce market imbalances.

Initially introduced as an individual right under Article 20 of the GDPR, data portability was aimed at enhancing user autonomy by enabling the secure and seamless transfer of personal data between service providers. However, recent regulatory developments have significantly expanded its scope. The Digital Markets Act (DMA) imposes data portability obligations on powerful digital platforms, or "gatekeepers," requiring real-time and effective data access for users and third parties. Similarly, the Data Act (DA) broadens the concept by including both personal and non-personal data, mandating standardized formats and access protocols to promote interoperability. Together, these instruments reflect a shift from a purely user-centric right to a broader regulatory tool designed to foster competition, reduce lock-in effects, and promote fair data sharing in digital markets.[3]

Despite the growing presence of data portability provisions in various regulatory frameworks, there remains a considerable disconnect between the theoretical potential of these rights and their real-world effectiveness. Article 20 of the GDPR, though a landmark provision in recognizing individual rights to data portability, is hindered by important limitations related to its narrow scope, technical feasibility, and weak enforcement mechanisms. These shortcomings are especially evident in competitive markets, where dominant firms can leverage their technical advantages and market power to undermine the practical impact of data portability, thereby weakening its role as a tool for promoting user mobility and market entry.

[3] Yongle Chao and others, 'Data Portability Strategies in the EU: Moving Beyond Individual Rights' (SSRN, 2024) 3–4 <https://www.ssrn.com/abstract=4933201> accessed 16 June 2025.

Against this backdrop, this thesis addresses the central research question: How can data portability rights be effectively enforced to achieve their intended objectives of enhancing user autonomy and promoting market competition?

This primary research question gives rise to several subsidiary areas of inquiry that structure the analytical framework of this study. The research examines the inherent limitations of the current data portability framework under the GDPR and analyzes how these constraints affect practical implementation in digital markets. It explores the extent to which competition law remedies can complement or supersede data protection mechanisms in ensuring effective data portability, particularly in circumstances where individual rights-based approaches prove insufficient. The study investigates how different legal systems approach the intersection of data portability and competition concerns, drawing comparative lessons from jurisdictions that have adopted varying regulatory strategies.

This thesis employs a comparative legal analysis as its primary methodological approach, examining how data portability is conceptualized, regulated, and enforced across different legal systems and regulatory domains.

The jurisdictional analysis focuses on the European Union and Turkey**,** offering insights into how different legal traditions and market contexts shape the development and implementation of data portability frameworks. Accordingly, Turkish Competition Authority's innovative approach in the *Sahibinden* case demonstrates how competition law can step in to address data portability concerns even in the absence of specific data protection provisions.

In this study, the regulatory framework of data portability under EU law will first be examined. In this context, particular emphasis will be placed on the GDPR, and alongside its legal framework, the conceptual limitations of the GDPR related to data portability will also be

discussed. Furthermore, the thesis will address the Digital Markets Act and the Data Act, which also regulate data portability under the broader EU framework. Following the explanation of the EU legal framework, attention will turn to competition law remedies in order to provide a clearer understanding of how data portability can function as such a remedy. The thesis will then explore the legal framework of data protection in Turkish law and the place of data portability within that framework to enable a comparative analysis. After outlining the Turkish legal framework, the thesis will analyze the decision of the Turkish Competition Authority in which data portability was imposed as a behavioral remedy in the *Sahibinden* case, offering a critical evaluation of that decision. Ultimately, by bringing together both regulatory and competition law perspectives from EU and Turkish legal systems, this study aims to offer a comprehensive assessment of data portability as a legal and strategic tool.

DATA PORTABILITY UNDER EU LEGAL FRAMEWORK

The Legal Framework of Article 20 of GDPR

The Right to Data Portability**,** introduced under Article 20 of the General Data Protection Regulation (GDPR) in 2018, was designed to promote greater fairness in digital markets. Its primary objective is to allow individuals to seamlessly and securely transfer their personal data between different service providers**,** and to reuse that data without limitations. Data portability refers to the right of individuals to retrieve and transfer their personal data between digital services in a structured, commonly used, and machine-readable format.[4] The right to data portability, introduced under Article 20 of the General Data Protection Regulation (GDPR), represents a novel legal mechanism designed to empower individuals in the digital environment by granting them greater control over their personal data. As highlighted by the Article 29 Working Party, this right is closely tied to the principles of data minimisation and user empowerment, and it holds the potential to support user switching and enhance competition by reducing data-based lock-in.[5] While its primary objective is grounded in data protection law, the right to data portability has also sparked broader legal and economic discussions, including its intersections with sector-specific regulation and market dynamics.[6]

Article 20 of the GDPR is comprised of two core entitlements: first, the right of the data subject to receive personal data concerning themselves which they have provided to a data controller, in a structured, commonly used and machine-readable format; second, the right to transmit that data to another controller without hindrance from the original controller, where technically

[4] OECD, *Data Portability and Interoperability*, 10.
[5] 'Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability (WP 242 Rev.01)' 7 <https://ec.europa.eu/newsroom/article29/items/611233>.
[6] Aysem Diker Vanberg and Mehmet Bilal Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo*'* (2017) 8 *European Journal of Law and Technology* 1, 2.

feasible.[7] This right applies exclusively to personal data processed by automated means and only when the processing is based on either the data subject's consent or a contract to which the data subject is a party. Thus, it excludes data processed on legal obligation, public interest, or the exercise of official authority, as well as manual or paper-based records.[8]

Crucially, the scope of the right is limited to data "provided by" the data subject. According to the Article 29 Working Party, this includes not only data actively and knowingly submitted by the user such as contact details or profile information but also observed data collected by virtue of the individual's use of a service, including location data, search history, and activity logs.[9] However, the right explicitly excludes inferred or derived data such as user profiles generated through algorithmic analysis or predictive scoring which are often considered commercially sensitive and the product of proprietary analytics. This exclusion reflects a balance between enabling individual empowerment and protecting trade secrets and intellectual property.[10]

The GDPR also places procedural obligations on data controllers. Under Article 12(3), controllers must respond to data portability requests without undue delay and in any case within one month, with the possibility of a two-month extension in complex cases.[11] The service must be provided free of charge unless the request is manifestly unfounded or excessive.[12] The data must be supplied in a format that is "structured, commonly used and machine-readable," a standard that implies technical accessibility but not full interoperability.[13] Recital 68 of the GDPR recommends that data controllers work towards creating formats that can work with

[7] '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 (General Data Protection Regulation) 95/46/EC [2016] OJ L119/1.'
[8] Article 29 Working Party, Guidelines on the Right to Data Portability, 8-9.
[9] *Ibid* 9–10
[10] Diker Vanberg and Ünver, *Right to Data Portability*, 5.
[11] GDPR, art 12(3).
[12] GDPR, art 12(5).
[13] Article 29 Working Party, *Guidelines on the Right to Data Portability*, 17–18.

other systems, but it doesn't make this a legal obligation. This means that even though the GDPR tries to make it easier for users to switch between services, it doesn't require companies to make their systems fully compatible. [14]

Ultimately, the legal framework of Article 20 GDPR establishes a foundational—but still developing—mechanism for individual data control, grounded in consent-based or contractual data processing, and defined by a relatively narrow interpretation of "provided" data. Its effectiveness in practice is contingent not only on legal interpretation but also on technical implementation and the development of standardised formats and procedures across sectors.

Conceptual Limitations and Regulatory Weaknesses of Article 20 of GDPR

The right to data portability under Article 20 of the GDPR was introduced as a tool to strengthen individual control over personal data and foster competition in digital markets. However, its practical implementation reveals several legal, technical, and economic challenges. This section explores the key limitations of Article 20, focusing on issues such as the unclear scope of applicable data, potential infringements on third-party privacy and intellectual property rights, and the disproportionate burden it places on small and medium-sized enterprises.

One of the most prominent limitations of the right to data portability under Article 20 of the GDPR is the uncertainty surrounding the scope of data it actually covers. Although the provision aims to enhance individuals' control over their personal data, it does not clearly define what types of data fall within its scope. This lack of clarity creates difficulties not only in terms

[14] Barbara Engels, 'Data Portability among Online Platforms' (2016) 5(2) *Internet Policy Review* 3–4 <https://policyreview.info/articles/analysis/data-portability-among-online-platforms> accessed 10 June 2025.

of implementation by data controllers but also for data subjects in understanding whether, and to what extent, they can invoke this right.

The GDPR itself states that the right to portability applies to personal data "provided by the data subject". However, the term "provided" is not fully explained in the regulation, and its interpretation significantly impacts the breadth of the right. According to the EDPB, the right to data portability should extend not only to data actively and knowingly provided by the data subject such as name or email address, but also to "observed" data which includes information such as search history, location data, or heart rate readings from wearable devices. On the other hand, inferred or derived data such as credit scores or algorithmically generated user profiles are not included within the scope of the right.[15]

This lack of clarity also has implications for determining who can benefit from the right. Since Article 20 applies only to personal data processed on the basis of consent or contract, individuals whose data is processed under a legal obligation or public interest basis are excluded.[16] In practical terms, this significantly narrows the class of eligible data subjects and complicates the identification of those who can realistically benefit from the right.

One of the other key limitations of the right to data portability under Article 20 of the GDPR is that its exercise may interfere with the privacy rights of individuals other than the data subject requesting the transfer. Article 20(4) clearly states that the right to portability 'shall not adversely affect the rights and freedoms of others'. This becomes particularly relevant in cases where the data requested by a user contains information about third parties who have not given their consent to such processing.[17]

[15] Jan Krämer, Pierre Senellart and Alexandre de Streel, *Making Data Portability More Effective for the Digital Economy* (CERRE, June 2020) 6 https://ssrn.com/abstract=3866495 accessed 30 May 2025.
[16] Krämer, Senellart and de Streel, *Making Data Portability More Effective*, 20.
[17] *Ibid* 22.

Moreover, in digital environments such as social media, where data is often inherently relational, applying this limitation becomes even more complicated. For instance, when multiple individuals appear in a photo or contribute to the same online content, the portability of data by one user could infringe upon the rights of others.[18] Additionally, porting personal data to services with lower privacy standards might allow individuals to bypass protections that were initially put in place by the original platform.

According to the Article 29 Working Party third-party data should remain under the exclusive control of the requesting data subject and not be processed by the receiving controller for their own purposes such as marketing or profiling.[19] Although this significantly limits the practical utility of such data for service providers; proposed solutions like technical filters and consent frameworks creates challenges in complex data environments.[20]

Another limitation in relation with privacy concerns of data portability relates to the quality and completeness of the data that can be transferred. Due to the privacy rights of third parties, some personal data cannot be ported in full, which may result in fragmented datasets. This limitation can negatively affect both the data subject and the recipient platform. The data subject may be unable to transfer all of their personal information to the new service, thereby hindering their ability to fully benefit from the right to data portability. At the same time, the receiving platform may encounter difficulties in processing the incomplete data, particularly if the missing elements relate to interactions or content shared with other users. As noted in the literature, data that is incomplete due to privacy or ownership concerns is generally of lower value, especially when important contextual information is missing.[21]

[18] Diker Vanberg and Ünver, *Right to Data Portability*, 3.
[19] Article 29 Working Party, *Guidelines on the Right to Data Portability*, 11–12.
[20] Krämer, Senellart and de Streel, *Making Data Portability More Effective*, 6–7.
[21] OECD, *Data Portability, Interoperability and Digital Platform Competition*, 25–26.

Another obstacle of Article 20 of the GDPR is its practical implementation poses considerable challenges particularly for small and medium-sized enterprises (SMEs). The requirement to enable structured, commonly used, and machine-readable export of personal data often entails the development of costly export-import modules (EIMs), application programming interfaces (APIs), and secure transfer mechanisms. For many SMEs, these technical requirements are disproportionately burdensome, especially when compared to the resources available to large platforms.[22] Some researchers point out that big online platforms can usually handle the costs and technical work needed to offer data portability. However, for smaller companies, these costs are much harder to manage especially since they do not have the same advantages from operating at a larger scale. These compliance challenges translate into broader economic consequences. When only large platforms can afford to meet regulatory obligations, the result is a distortion of competition. SMEs are not only discouraged from entering data-driven markets but may also be pushed out of existing ones.[23] This leads to a classic entry barrier, which is contrary to the GDPR's pro-competition goals and risks entrenching the dominance of incumbent platforms.

Moreover, non-compliance with portability requirements contributes directly to consumer lock-in. When data cannot be ported easily, users are less likely to switch services, even when viable alternatives exist. This issue becomes even more serious in markets with strong network effects namely social media or cloud services where the usefulness of the platform grows as more people use it. When users cannot easily move their data like their contacts, reputation scores, or activity history to another service, they become more tied to the original platform. As Krämer et al. suggests the GDPR's vision of user autonomy remains unrealized unless data portability is supported by interoperability and continuous, real-time access to user-generated

[22] Diker Vanberg and Ünver, *Right to Data Portability*, 4.
[23] Johann Kranz and others, 'Data Portability' (2023) 65(5) *Business & Information Systems Engineering* 597–600 https://doi.org/10.1007/s12599-023-00815-w accessed 10 June 2025.

data.[24] Without these technical enablers, the right to portability remains underutilized and fails to promote the competitive mobility.

Another significant concern for right to data portability is that under Article 20 of the GDPR aims to enhance user control over personal data, it also creates potential conflict with intellectual property rights. As personal data gains economic importance in digital markets, there is growing legal and commercial concern that data portability requests could interfere with protected proprietary information.

The GDPR seeks to strike a balance between empowering users and protecting the rights and freedoms of others. Article 20(4) explicitly states that the right to data portability must not adversely affect such rights. However, it does not expressly mention intellectual property or trade secrets in this context. Even tough Article 20(4) does not specifically point out the intellectual property rights, Recital 63 of GDPR concerning the general right of access does refer to the need to protect intellectual property. Some scholars argue that this limitation should also apply to Article 20.[25]

A core issue lies in the unclear boundary between personal data and proprietary datasets. Many digital services generate valuable insights or structures through a combination of user input and proprietary algorithms. For instance, Spotify is a personalized music streaming service that builds unique playlists based on user-provided data such as name, age, gender, and location; observed data such as listening history and the duration and frequency of sessions; and inferred or derived data such as genre and mood preferences. If this platform were required to transfer all of this user data to a rival platform, it could expose not only raw personal data but also proprietary recommendation algorithms and tailored content selections that form a core part of

[24] Krämer, Senellart and de Streel, *Making Data Portability More Effective*, 9.
[25] Diker Vanberg and Ünver, *Right to Data Portability*, 5; GDPR, art 20(4).

the company's competitive edge. In such a case, the portability request risks disclosing elements that are closely tied to the platform's intellectual property and business model.

Data Portability Under Digital Markets Act (DMA)

The Digital Markets Act introduces a significant evolution in the regulatory approach to data portability, expanding beyond the GDPR's framework to address specific competitive concerns in digital markets. Article 6(9) DMA obligates gatekeepers to provide end users with 'effective portability of data provided by the end-user or generated through the activity of the end user'. [26] This provision represents a notable departure from the GDPR's more restrictive approach, both in scope and implementation requirements.

The DMA's data portability provisions differ from the GDPR framework in several crucial respects. While the GDPR limits portability to personal data explicitly provided by data subjects under consent or contractual arrangements, the DMA encompasses both personal and non-personal data generated through user activity on gatekeeper platforms.[27] This broader scope reflects the DMA's recognition that effective competition in digital markets requires access to comprehensive datasets that may include inferred and derived data previously excluded from GDPR protections.[28]

However, the effectiveness of the DMA's data portability regime remains contingent upon its interaction with interoperability measures within the same regulation.[29] As Lazarotto observes,

[26] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1, art 6(9).
[27] Bárbara da Rosa Lazarotto, 'The Right to Data Portability: A Holistic Analysis of GDPR, DMA and the Data Act' (2024) 15(1) *European Journal of Law and Technology* 8 https://ejlt.org/index.php/ejlt/article/view/984 accessed 10 June 2025.
[28] Florian Hey, *'Data interoperability and portability in the DMA: Competition booster or lame duck?'* (Ilmenau University of Technology 2024) Ilmenau Economics Discussion Papers No 192, 6.
[29] OECD, *Data Portability, Interoperability and Digital Platform Competition*, 49.

the impact of data portability 'is highly dependent on the effectiveness of the established interoperability regime'.[30] This interdependence suggests that data portability alone may be insufficient to achieve the DMA's competitive objectives without complementary measures ensuring technical compatibility between platforms.

Data Portability Under Data Act (DA)

The Data Act represents a further evolution in European data portability frameworks, extending beyond personal data protection to establish comprehensive access rights in IoT ecosystems. Unlike the GDPR's focus on personal data or the DMA's emphasis on gatekeeper platforms, the Data Act creates horizontal access rights covering 'data generated by the use of the product or related services' across connected devices.[31]

Articles 4 and 5 of the Data Act establish a two-tiered access framework. Article 4 grants users direct access to data generated through product use, while Article 5 enables users to share this data with third parties.[32] The Act mandates that data be made available 'without undue delay, free of charge, easily, securely, in a structured, commonly used and machine-readable format, continuously and in real-time'.[33] This technical specification mirrors the DMA's real-time requirements while extending to a broader range of connected products.

Importantly, the Data Act departs from the conventional distinction between personal and non-personal data by covering "all data generated including personal and non-personal data by the use of a product or related service." Its broad scope encompasses both intentionally and

[30] Lazarotto, *Right to Data Portability*, 7–9.
[31] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data (Data Act) [2023] OJ L, art 2(1).
[32] ibid, arts 4-5.
[33] ibid, art 4(1).

unintentionally collected data, such as diagnostics and information captured even while a device is in standby mode.[34]

The Data Act introduces the concept of 'data access by design', requiring IoT manufacturers to design products facilitating real-time, continuous data accessibility.[35] This proactive approach contrasts with the reactive frameworks of both GDPR and DMA, embedding portability considerations into product development from inception.

Despite these advances, Lazarotto identifies implementation challenges, noting that the Act's 'dubious language' creates uncertainty about whether users receive actual data copies or merely in-situ access.[36] This ambiguity potentially undermines the Act's portability objectives by maintaining data controller gatekeeping functions.

[34] ibid. Lazarotto, *Right to Data Portability*, 9-11.
[35] Data Act, art 3.
[36] Lazarotto, *Right to Data Portability*, 11.

DATA PORTABILITY IN COMPETITION LAW

Overview of Competition Law Remedies

In competition law, remedies play an important role in addressing the harm caused by anti-competitive practices and ensuring that markets remain fair and functional. These remedies are generally divided into two main types: structural and behavioral. Structural remedies usually involve more permanent changes to a company's structure. On the other hand, behavioral remedies are about regulating a company's future conduct. Each type has its own advantages and drawbacks. In recent years, especially with the rise of digital markets, there has been more debate about when each type of remedy should be used, or whether a mix of both might be more effective. Understanding the logic and impact of structural and behavioral remedies is essential for analyzing how competition authorities design interventions that truly promote competitive outcomes.

Structural remedies are defined as measures that effectively change the structure of a firm through the transfer of property rights regarding tangible or intangible assets, including the transfer of entire business units, without creating ongoing relationships between the former and future owner. A key distinguishing feature is that after implementation, structural remedies do not require further monitoring, as they remove both the incentive and the means for a firm to repeat competition law infringements.[37]

Structural remedies are generally seen as more effective than behavioral remedies because they target the root economic causes of anticompetitive practices, rather than just limiting how a firm behaves. After being implemented, they usually do not need constant monitoring, and they

[37] Frank P Maier-Rigaud, 'Behavioural versus Structural Remedies in EU Competition Law' in Philip Lowe, Mel Marquis and Giorgio Monti (eds), *European Competition Law Annual 2013: Effective and Legitimate Enforcement of Competition Law* (Hart Publishing 2016) 209-210.

work in harmony with market forces, making them a more sustainable solution for promoting competition in the long term.[38]

Although structural remedies have clear benefits, they also come with significant challenges. For instance, breaking up a company can disrupt its business model by removing efficiencies like economies of scale or scope. There is also the risk that the separated parts may not survive on their own or that no appropriate buyers can be found. Additionally, these remedies raise concerns about proportionality, as they involve altering property rights, which are legally protected. Finally, the process of designing and implementing structural remedies can be complex, time-consuming, and require substantial resources.[39]

Behavioral remedies are measures that constrain how a firm exercises its property rights by setting limits on business conduct or requiring specific actions.[40] Behavioral remedies can take various forms and are often classified based on whether they impose positive obligations such as requiring firms to take specific actions or negative ones such prohibiting certain types of conduct.[41] These remedies aim to adjust a firm's behavior in the market without altering its structure. Common examples include requiring companies to modify or terminate existing contracts, eliminate exclusivity clauses, implement new pricing schemes or conditions, and facilitate consumer switching between providers. Additionally, firms may be obliged to adopt compliance programs or provide competition law training, as well as amend their corporate governance frameworks to prevent future infringements.[42]

[38] OECD (2022), Remedies and commitments in abuse cases, *OECD Competition Policy Roundtable Background Note,* www.oecd.org/daf/competition/remedies-and-commitments-in-abuse-cases2022.pdf 208.
[39] Maier-Rigaud, 'Behavioural versus Structural Remedies', 208.
[40] ibid, 209
[41] OECD, *Remedies and Commitments in Abuse Cases*, 19–20.
[42] ibid 20

A fundamental characteristic of behavioral remedies is their requirement for permanent monitoring and enforcement because they do not eliminate the underlying incentive structure that led to the original infringement.[43]

Behavioral remedies offer several advantages over structural alternatives. They can be precisely tailored to address specific competitive concerns without fundamentally altering market structure.[44] This targeted approach may be particularly appropriate where the competition problem stems from specific conduct rather than market structure itself.

Unlike structural remedies, behavioral measures can preserve legitimate business efficiencies and economies of scale or scope that might be lost through divestiture.[45] This is particularly important where integration or coordination serves pro-competitive purposes alongside any potentially harmful effects.

In addition, behavioral remedies can be modified, updated, or terminated as market conditions change, providing greater flexibility than permanent structural changes.[46] This adaptability can be valuable in dynamic markets where competitive conditions evolve rapidly.

Behavioral remedies face several fundamental limitations that undermine their effectiveness in competition law enforcement. The most significant challenge is their requirement for ongoing monitoring and enforcement. This creates substantial administrative costs and resource demands that may exceed the capacity of many competition authorities. Behavioral remedies are often undermined by incentive problems, as they require firms to act against their own interests without removing the root causes of anticompetitive behavior. This leads firms to find ways to bypass the rules. Additionally, behavioral remedies are inherently inflexible in

[43] Maier-Rigaud, *'Behavioural versus Structural Remedies'*, 209–210.
[44] OECD, *Remedies and Commitments in Abuse Cases*, 19–20.
[45] ibid 17
[46] ibid 17

adapting to changing market conditions, as they are based on an existing understanding of the market at the time they are imposed. As markets evolve, these remedies may become ineffective or even counterproductive, especially given the fundamental uncertainty about future developments, which makes it difficult to design measures that remain suitable over time.[47]

Behavioral remedies remain the dominant form of intervention in competition law enforcement, particularly in abuse of dominance cases, where they are chosen significantly more frequently than structural alternatives. Competition authorities have historically viewed behavioral remedies as less intrusive and more proportionate responses to competition in abuse of dominance concerns, allowing them to address specific conduct without fundamentally altering market structure or ownership arrangements.

Data Portability as a Competition Law Remedy

Considering data portability as a behavioral remedy can be an important step forward in competition law, especially in digital markets where former antitrust methods often struggle to deal with new types of competition problems. In this context, data portability requirements emerge as a sophisticated regulatory instrument designed to reduce switching costs, enhance consumer choice, and lower barriers to entry for potential competitors.

In addition to its positive effects on data protection, privacy, and market structure as provided by Article 20 and discussed in earlier chapters, data portability can also function as an effective remedy under competition law in digital markets. The rationale for enforcing data portability as a competition tool closely aligns with the pro-competitive objectives underlying Article 20.

[47] Maier-Rigaud, *'Behavioural versus Structural Remedies'*, 210-211.

First, data has become a vital competitive asset; in markets shaped by strong network effects, the accumulation of large datasets can reinforce the dominance of established platforms. Second, users' inability to easily transfer their data between services creates artificial switching costs, insulating incumbents from competitive pressure. Third, mandating data portability and interoperability offers a comparatively less intrusive means of restoring competitive dynamics, as it reduces entry barriers without requiring structural changes to firms or market design.

Notably, despite the theoretical appeal of data portability as a competition remedy, the European Commission has not applied data portability requirements as a remedy in any of its competition enforcement cases to date.

Despite acknowledging the competitive significance of data portability, the Commission has maintained a notable gap between theory and practice, having not yet imposed a sanction on the basis of a failure to enable data portability. This enforcement gap reflects deeper uncertainties about when and how to mandate data portability as an effective remedy in competition cases. The most illustrative example of this cautious approach emerges from the Commission's treatment of Google's AdWords platform, where it expressed specific concerns regarding data portability restrictions that could harm competition. The Commission's analysis focused on how high costs of recreating advertising campaigns, combined with contractual or other restrictions hindering portability, could lead to the exclusion of equally efficient competitors from the online advertising market. However, despite these clearly articulated competitive concerns, the Commission notably refrained from imposing any sanctions, demonstrating its willingness to identify potential competitive infringements without taking concrete enforcement action.[48]

[48] Orla Lynskey, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability' (2017) 42 *European Law Review* 1-4.

The Commission's position on extending data portability beyond personal data reveals notable hesitation despite its general support for data economy development. The Commission acknowledges in its "Building a European Data Economy" Communication that effective data flow requires protection and views the GDPR as foundation to EU data flow.[49] However, it explicitly rejects broader data portability applications. Instead of introducing concrete measures for non-personal data, the Commission has chosen a consultative path, indicating that it will "invite stakeholders to explore whether this assessment can be generalized and to consider the potential negative impacts of a portability right for non-personal data in specific markets."[50]

The Commission's hesitation to introduce data portability as a remedy mainly comes from the limits of competition law, which are quite different from the more flexible and proactive approach seen in regulations like the GDPR. Competition law remedies for data portability can only be applied when dominance and abuse are conclusively established, creating a narrow enforcement framework that applies only to specific undertakings in particular circumstances rather than establishing general rights.[51]

Rather than mandating comprehensive data portability, the European Commission has demonstrated a clear preference for alternative remedial approaches, particularly interoperability requirements and data compartmentalization measures.

The Commission's approach to interoperability remedies is most clearly illustrated in its landmark Microsoft decision, which established important precedents for how competition authorities can address data and information access issues in digital markets. In its 2004

[49] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy* COM(2017) 5, 10 January 2017.
[50] ibid, 17.
[51] Lynskey, *Aligning data protection rights with competition law remedies?,*6.

decision, the Commission found that Microsoft had abused its dominant position by refusing to supply technical information necessary for competitors to provide certain software for networking computers.[52]

The Commission's remedy was both comprehensive and precisely targeted. Instead of demanding that Microsoft make all its data portable or accessible, it required the company to share complete and accurate documentation of the protocols used by Windows work group servers. This information had to be made available promptly and under fair, reasonable, and non-discriminatory conditions. Crucially, the decision specified that any remuneration charged for access to this information should not reflect "strategic value" stemming from Microsoft's market power, and should not restrain innovation or create disincentives to compete with Microsoft.[53]

This approach demonstrates the Commission's preference for surgical intervention rather than broad structural changes. The remedy was designed to address the specific competitive harm by the exclusion of competitors from the work group server operating systems market without fundamentally altering Microsoft's business model or requiring comprehensive data sharing across all its operations.

[52] Commission Decision 2007/53/EC of 24 March 2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft) [2007] OJ L32/23
[53] OECD, *Data Portability, Interoperability and Digital Platform Competition*, 29-30.

TURKISH LEGAL CONTEXT

Turkish Data Protection Framework and Its Alignment with GDPR

Turkey's Personal Data Protection Law No. 6698, known as *Kişisel Verileri Koruma Kanunu* (KVKK), came into force on 7 April 2016. The KVKK represents Turkey's first comprehensive data protection law and was specifically designed to align Turkish legislation with EU standards, particularly EU Directive 95/46/EC, which governed data protection in the European legislation before the GDPR. While both laws share fundamental objectives and principles, significant differences exist, particularly regarding data portability rights.

Both the KVKK and the GDPR regulate how personal data is processed by natural and legal persons, but they differ notably in terms of territorial scope. The KVKK applies to all data controllers and processors that collect or handle personal data obtained from within Turkey, covering both domestic entities and foreign organizations processing data related to individuals in Turkey.[54] In contrast, the GDPR has a wider extraterritorial scope, extending its application to entities outside the EU if they provide goods or services to individuals in the EU or track their behavior.[55]

A key difference lies in registration requirements. Unlike the GDPR, the KVKK mandates that all data controllers register with the Data Controllers' Registry (VERBIS) before beginning processing operations, regardless of their size or annual turnover.[56] This reflects a stricter

[54] Endpoint Protector, 'All You Need to Know About Turkey's Personal Data Protection Law (KVKK)' (2023) https://www.endpointprotector.com/blog/everything-you-need-to-know-about-turkeys-personal-data-protection-law/ accessed 15 January 2025.
[55] GDPR art. 3
[56] Law No 6698 on the Protection of Personal Data (KVKK), adopted 24 March 2016, Official Gazette No 29677, 7 April 2016, art 16.

stance than the GDPR, which focuses more on internal documentation and the principle of accountability by the data controller.

Both regulations are built upon similar fundamental principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity.[57] However, the GDPR explicitly includes accountability as a principle, which is not directly addressed in the KVKK.

The KVKK grants data subjects a range of rights similar to those under the GDPR, such as the right to be informed about how their data is processing, the right to access to personal data, as well as the right to rectification, the right to erasure, the right to restriction of processing.

However, critical differences emerge when examining specific rights. The KVKK relies more heavily on explicit consent as the primary legal basis for processing, treating other conditions as exceptions, whereas the GDPR treats all legal bases equally.[58] This represents a more consent-centric approach in Turkish law.

One of the most significant gaps between the KVKK and the GDPR is the absence of a provision on data portability in the Turkish framework. Unlike Article 20 of the GDPR, which explicitly grants individuals the right to receive and transfer their personal data between controllers, the KVKK does not include an equivalent right.

While the KVKK does not contain a general provision on data portability, one example of sector-specific data portability regulation in Turkey is the Number Portability Regulation (Numara Taşınabilirliği Yönetmeliği). The Number Portability Regulation allows subscribers

[57] 21 Analytics, 'Citizen's Data Protection: the EU's GDPR and Türkiye's KVKK' (2025) https://www.21analytics.ch/blog/gdpr-and-kvkk-compared/ accessed 15 January 2025.
[58] Mondaq, 'Gap Analysis: GDPR vs Turkish Personal Data Protection Law (KVKK)' (2018) https://www.mondaq.com/turkey/privacy-protection/724120/gap-analysis-gdpr-vs-turkish-personal-data-protection-law-kvkk accessed 15 January 2025.

to 'change the operator they receive service from without changing their number,' enabling 'operator number portability.[59] The Number Portability Regulation represents a sectoral approach to portability, limited to telecommunications services. This contrasts sharply with the GDPR's comprehensive approach to data portability, which applies across all sectors within the regulation's scope.

Overall, the comparison between the KVKK and GDPR reveals significant differences in their approach to data portability. While the GDPR establishes a comprehensive right to data portability as part of its framework for individual control over personal data, the KVKK contains no equivalent provision. Turkey's only regulation of data portability occurs in the telecommunications sector through its Number Portability Regulation, which demonstrates understanding of portability's competitive benefits but fails to extend these protections to other digital services.

The Application of Data Portability In Turkish Competition Law: Sahibinden Decision

While data portability has primarily been discussed as a right under the GDPR, its practical relevance is increasingly acknowledged within the context of competition law. Although data portability is not defined as a right under the KVKK, the Turkish Competition Authority (TCA) has nevertheless recognized its potential as a remedy to address anticompetitive practices. A prominent example is the TCA's decision concerning the online real estate platform *Sahibinden*, where the Authority imposed data portability obligations as a structural remedy to tackle competition concerns. This case illustrates how data portability can be employed not

[59] *Numara Taşınabilirliği Yönetmeliği*, Official Gazette, 2 July 2009, No 27276.

only as a tool for enhancing data protection, but also as a means to correct market imbalances and lower entry barriers, even in jurisdictions where it is not explicitly codified as a right.

Data Portability as a Remedy: Insights from the Turkish Competition Authority's Sahibinden Case

On 23 August 2023, the TCA published its final decision against *Sahibinden Bilgi Teknolojileri Pazarlama ve Ticaret A.Ş.* (Sahibinden), finding that the company had abused its dominant position in the market for vehicle sales and rental platform services. The TCA concluded that *Sahibinden* had violated Article 6 of Law No. 4054 on the Protection of Competition by restricting data portability and enforcing exclusivity through non-compete clauses in its contracts with business users. As a result, the authority imposed both administrative fines and structural remedies aimed at restoring competitive conditions, including a novel data portability obligation.

Founded in 2000, *Sahibinden.com* is a digital platform that connects individuals and businesses wishing to post classified ads or sell products and services with potential consumers. The platform operates across ten major categories, including real estate, vehicles, industrial equipment, services, job listings, pets, and consumer goods. However, its core business focus lies primarily in real estate sales and rentals, as well as vehicle listings.

Sahibinden employs two main business models. The first is a classified ads model where sellers can post listings and potential buyers contact them directly using the information provided (such as name and phone number). In this model, *Sahibinden* acts purely as an intermediary and does not participate in or track the transaction itself. The second is an e-commerce marketplace model which is applied mainly in the second-hand and spare parts and accessories categories. Here, the platform facilitates the transaction between buyers and sellers and collects

a commission from the seller for its intermediation services. In both cases, *Sahibinden* does not set prices or influence the terms of sale.[60]

In its assessment, the TCA defined the relevant product markets as 1) online platform services for real estate sales and rentals by business users, and 2) online platform services for vehicle sales by business users. Individual users were excluded from the analysis since their limited and irregular listing activity did not raise data portability concerns.[61]

The relevant geographic market is defined as Turkey by TCA**,** noting that the platform services in question do not vary regionally and can be accessed by users like car dealers or real estate agencies from any location with internet access.[62]

According to the TCA's evaluation, *Sahibinden* held a significantly higher market share than its competitors in 2021. This results in a disproportionate share of revenue from business users and maintains a stronger position in terms of pricing power and market influence.[63]

TCA found that *Sahibinden* engaged in several exclusionary practices that reinforced its dominant position and restricted competition in the market for online platform services for real estate and vehicle listings. A central concern was the platform's obstruction of data portability which is assessed by TCA as a key barrier to multi-homing referring to the ability of business users (such as real estate agencies and car dealerships) to operate on more than one platform simultaneously.

[60] Turkish Competition Authority, *Sahibinden Bilgi Teknolojileri Pazarlama ve Ticaret A.Ş. Decision* (23 August 2023) Case No 23-39/765-263, para 11-12 https://www.rekabet.gov.tr/Dosya/sahibinden-nihai-kararr.pdf accessed 31 May 2025.
[61] ibid, paras 31-41.
[62] ibid, paras 42-43
[63] ibid, paras 95-102

Specifically, *Sahibinden* did not provide its business users with any practical means to extract or transfer their listings and related data namely images, descriptions, prices, and customer contact details to other platforms. The company also failed to offer access to data through an open API, further preventing seamless data transfer and automated integration with competing services. This lack of portability not only made it costly and time-consuming for users to duplicate their content elsewhere but also resulted in a form of de facto exclusivity. In the TCA's view, this amounted to a restriction of user mobility, which contributed to market foreclosure by raising the switching costs for businesses and entrenching *Sahibinden's* dominance.[64]

In addition to restricting data transfer, *Sahibinden* imposed de facto exclusivity through contractual non-compete clauses that prevented business users from collaborating with rival platforms. The platform also restricted the number of sub-users under a single business account, complicating agency workflows and making it difficult for larger real estate agencies to manage listings across multiple platforms.[65]

Further concerns arose from *Sahibinden's* lack of transparency in advertising, particularly in how it published promoted and native advertisements. The decision noted that the platform appeared to self-preference its own services through algorithmic rankings, raising concerns about biased visibility and market foreclosure. Additionally, services such as vehicle valuation, real estate price estimation, and referrals to authorized dealers were found to disproportionately favor *Sahibinden*, potentially distorting user choice and fair competition.[66]

In its legal assessment, TCA concluded that *Sahibinden* imposed extensive contractual and technical barriers that effectively prevented business users from transferring their own listing

[64] ibid, paras 128
[65] ibid, paras 174-199
[66] ibid, paras 479-498

data to competing platforms. Several provisions in *Sahibinden's* corporate membership agreements prohibited the reproduction, processing, or transfer of any platform content including users' own listing data under broad and ambiguously worded clauses. These terms were interpreted as restricting both the outbound transfer of data to rival platforms and the inbound import of listings from external sources. The TCA found that these restrictions applied even when users sought to transfer their data voluntarily or through third-party integration services.[67]

In addition to contractual and technical restrictions, the TCA's analysis highlights how *Sahibinden's* obstruction of data portability exacerbated structural challenges already present in the online platform markets for real estate and vehicle listings. Business users especially real estate agents and car dealers faced practical burdens when trying to upload and maintain listings across multiple platforms. These burdens, such as time-consuming duplicate entry, increased operational costs and discouraged multi-homing. Despite attempts by rival platforms to support data integration and offer easier listing tools, these efforts often failed due to *Sahibinden's* refusal to cooperate or enable interoperability.

The TCA found that *Sahibinden's* restrictions on data portability had tangible anti-competitive effects, particularly by limiting multi-homing opportunities for business users and weakening the competitive position of rival platforms. Most users were observed to operate exclusively on *Sahibinden*, despite showing motivation to use alternative platforms. This exclusivity stemmed not from user preference alone, but from the technical and contractual barriers that made parallel usage costly, inefficient, or impractical. Even when rival platforms offered

[67] ibid, paras 808

lower-priced listing packages, business users continued to concentrate their listings on *Sahibinden* due to difficulties in transferring and updating content across platforms.[68]

To address these issues, the TCA outlined a technical remedy that would enable business users to transfer their listing data via secure download formats or through token-based APIs without compromising platform integrity or proprietary enhancements.

Following its finding that *Sahibinden* had abused its dominant position by restricting data portability and thereby raising barriers to multi-homing, the TCA imposed a set of structural and behavioral remedies aimed at restoring competitive conditions in the market. First, the TCA required *Sahibinden* to revise its contracts with business users within three months of receiving the reasoned decision. The new contracts must exclude clauses that directly or indirectly restrict data portability or enforce exclusivity.

More importantly, the TCA required *Sahibinden* to develop the necessary technical infrastructure free of charge. This infrastructure must enable business users to seamlessly transfer the data they input on the platform such as photos, listing details, and contact information to competing platforms.

This obligation does not only cover transferring data just but also means that making sure the data stays updated on all platforms. Also, if business users want to bring their data from other platforms into *Sahibinden,* and those platforms agree, *Sahibinden* must help with the transfer quickly and smoothly.

[68] [68] ibid, paras 371-394

To ensure compliance, *Sahibinden* is also subject to a long-term reporting obligation: it must notify the TCA once the compliance measures have been implemented and submit annual progress reports for a period of three years. [69]

These remedies mark a significant development in the intersection of competition enforcement and data governance, explicitly recognizing the centrality of data portability not only as a consumer right under the GDPR, but also as a tool to foster platform competition.

Assessment of the Limits of Article 20 of GDPR on Right to Data Portability Through the Sahibinden Decision

The right to data portability, enshrined in Article 20 of the GDPR, was introduced as a mechanism to enhance user control over personal data and facilitate competition by reducing switching costs between digital services. While conceptually promising, its effectiveness has been questioned due to its limited scope and dependence on user consent. These limitations are particularly problematic in data-driven markets where strong network effects and technical lock-ins suppress competition and entrench market power. This section examines the Turkish Competition Authority's (TCA) decision in the *Sahibinden* case as a pivotal example of how competition law can complement and in certain respects, surpass the GDPR by imposing concrete, enforceable obligations that enable functional data mobility. By analyzing the behavioral remedies mandated by the TCA and their implications, the discussion highlights how competition enforcement can bridge the regulatory gaps left by data protection frameworks.

[69] ibid, para 817

To begin with, a key driver behind the TCA's innovative approach in the *Sahibinden* case was the lack of a comprehensive data portability framework in Turkish law. Unlike the European Union, where data portability is explicitly recognized under Article 20 of the GDPR, Turkey's Personal Data Protection Law (KVKK) does not provide a general right to data portability. As a result, conventional data protection tools were insufficient to address the competitive issues at stake in this case. The absence of data portability provisions in Turkish data protection law prompted the TCA to rely on competition law mechanisms, leading to the adoption of broader and potentially more effective remedies than what would have been possible through data protection enforcement alone.

Moreover, The *Sahibinden* decision illustrates how competition law can complement the GDPR by enforcing data portability remedies even for data types and processing scenarios not covered under Article 20 of GDPR.

The *Sahibinden* decision by the Turkish Competition Authority (TCA) serves as a compelling illustration of how competition law can compensate for the limitations of the GDPR's Article 20 right to data portability. According to the GDPR, the portability right is restricted to personal data actively provided or passively observed by the data subject, and only when the processing is based on consent or a contract. Inferred or derived data, as well as data processed under legal obligations or public interest grounds, fall outside this scope.[70] This narrow interpretation reduces the effectiveness of Article 20 in addressing structural market failures, especially in data-driven digital markets with high switching costs.

These restrictions significantly inhibited data mobility and created lock-in effects that prevented multi-homing. Recognizing this situation as an abuse of dominance, the TCA

[70] Krämer, Senellart and de Streel, *Making Data Portability More Effective*, 19–20.

imposed behavioral remedies that went beyond the GDPR framework. Sahibinden was ordered to establish, at no cost to users, a technical infrastructure that would allow business users to seamlessly port their listing data including descriptions, images, and contact details to rival platforms and keep that data updated. Moreover, the remedy required the platform to accept incoming data from competitors when requested by users, provided that rival platforms agreed to such transfers.[71]

This regulatory approach is particularly significant because it enables the portability of data that may not be covered by Article 20 either because it lacks the legal basis of consent/contract, or because it does not constitute personal data. In doing so, the TCA not only closed the enforcement gap left by the GDPR but also created a more competition-oriented portability regime.

The *Sahibinden* case thus highlights the practical limitations of a consent-based portability framework and shows how competition authorities can step in with structural and behavioral remedies to secure meaningful data mobility.

Secondly, even though main aims of the data portability right under GDPR includes enhancing consumer autonomy and reduce lock-in effects by facilitating switching behavior, the enforcement of this right may remain motionless considering the fact that the right is inherently contingent upon user consent meaning that its practical effectiveness is entirely dependent on individuals choosing to exercise it. This limitation is highly crucial in contexts where the lack of portability contributes to entrenched market power and forecloses competition. In such cases, as in the *Sahibinden* decision, it is important for competition authorities to identify the issue and impose various remedies to address this shortcoming.

[71] TCA, *Sahibinden*, para 817.

The limitations of consent-based data portability become particularly evident in markets where the lack of effective data transfer mechanisms contributes to entrenched dominance and restricts competition. The *Sahibinden* decision issued by the TCA offers a compelling illustration of this dynamic. In its assessment, the TCA found that *Sahibinden* implemented both contractual and technical restrictions that hindered real estate professionals from transferring their listings and related data. This data includes property descriptions, images, and customer details.[72] These practices significantly raised switching costs and obstructed multi-homing. Crucially, while the relevant data may qualify as personal data under Article 20 of the GDPR, the willingness of users to exercise their right to data portability would probably be insufficient to preserve competitive conditions in the market. In light of this, the TCA determined that regulatory intervention was necessary and imposed behavioral remedies designed to facilitate effective and fair data access for rival platforms, thereby addressing the underlying competition concerns.

Moreover, The GDPR's data portability right under Article 20 is rooted in privacy and data protection, not in the correction of market imbalances. Accordingly, the scope of the right is limited: it applies only to personal data that are either actively provided or passively observed, and only when the processing is based on the data subject's consent or a contractual relationship. This narrow framing reflects the GDPR's principal policy objective: it is designed to safeguard fundamental rights and ensure data security, not to promote competition in digital markets. [73]

This regulatory gap becomes more problematic in digital markets characterized by strong network effects and high switching costs, where user consent alone may not suffice to generate

[72] TCA, *Sahibinden*, para 203.
[73] Graef, *Putting the Right to Data Portability into a Competition Law Perspective*, 8–9.

meaningful competition.[74] In such contexts, competition law plays a complementary and at times corrective role. In *Sahibinden* case, the TCA not only acknowledged the platform's dominant position in the markets for online real estate and vehicle listings, but also found that *Sahibinden* had abused this dominance by obstructing the portability of listing data through contractual clauses, technical limitations, and refusal to enable integration with rival platforms.[75]

Crucially, the TCA did not merely encourage data mobility through general principles; it imposed concrete behavioral remedies under competition law. *Sahibinden* was required to establish free of charge a technical infrastructure allowing business users to transfer their data (including listing content, images, and contact information) to rival platforms, and to keep this data up to date. Moreover, the obligation extended bidirectionally: where business users wished to transfer their data into *Sahibinden* from other platforms, and where rivals agreed, *Sahibinden* was equally obliged to ensure a seamless and effective transfer.[76] These remedies were not framed as voluntary commitments but as legally binding obligations aimed at restoring competitive conditions in the market.

Importantly, the TCA's intervention in the *Sahibinden* decision also addressed one of the persistent shortcomings of the GDPR's right to data portability: the fragmentation of datasets due to privacy-related constraints. Under Article 20 of the GDPR, the right to portability is limited to personal data actively provided or passively observed by the user, and excludes inferred or derived data as well as any data that implicates third-party privacy unless additional consents are obtained. As a result, even when users attempt to exercise their right, the transferred dataset may be incomplete lacking key contextual or interactional elements thereby

[74] Krämer, Senellart and de Streel, *Making Data Portability More Effective*, 56-57.
[75] TCA, *Sahibinden*, para 811.
[76] ibid, 817.

limiting its utility for re-use and reducing its competitive value. This limitation is particularly acute in data-rich markets, where meaningful switching between platforms depends on the ability to port full, functional datasets.[77]

In contrast, the TCA's remedy-based approach bypassed this limitation by reconfiguring data portability as a competition remedy rather than a privacy-based individual right. By identifying *Sahibinden*'s conduct namely, the prevention of data portability through contractual and technical restrictions as an abuse of dominance, the authority imposed behavioral remedies that directly targeted the anti-competitive effects of data lock-in. Specifically, *Sahibinden* was obligated to implement a technical infrastructure (based on an API mechanism) that enables business users such as real estate agencies and car dealers to seamlessly transfer all listing data, including images, prices, descriptions, and contact details, to rival platforms without cost and without fragmentation.[78] Crucially, this data transfer mechanism was not subject to individual user consent or limited by the potential privacy claims of third parties, since the TCA framed the remedy as a structural market correction tool rather than a voluntary data subject right.

This shift in legal framing allowed the transferred data to retain its completeness and relevance, thereby overcoming the typical limitations imposed by privacy concerns. The economic and competitive utility of data portability is significantly diminished when the transferred data is incomplete or fragmented due to privacy-related exclusions. [79] The *Sahibinden* case illustrates that competition law can step in to ensure that data mobility occurs in a meaningful and actionable way, facilitating lower switching costs, promoting multi-homing, and restoring competitive balance in markets characterized by strong network effects and entrenched incumbents. In this sense, the TCA's decision demonstrates how behavioral remedies rooted

[77] OECD, *Data Portability, Interoperability and Digital Platform Competition*, 17-18.
[78] TCA, *Sahibinden*, para 817.
[79] Engels, *Data Portability among Online Platforms*, 4–5.

in competition law can serve as a functional complement to the GDPR, effectively filling in the enforcement gaps and ensuring that data portability contributes not only to user empowerment, but also to market-level contestability.

In sum, the Sahibinden decision underscores the critical role competition law can play in reinforcing and expanding the practical reach of data portability. By framing restrictions on data transfer as an abuse of dominance, the TCA not only addressed structural barriers to competition but also ensured that datasets potentially beyond the personal data protected under the GDPR could be ported in full, without fragmentation or consent-related limitations. This approach provides a valuable regulatory template for tackling similar challenges in other data-driven markets, where user-centric mechanisms under privacy law alone may fall short. The decision also signals a growing convergence between data protection and competition law, where behavioral remedies can be tailored to promote both individual rights and market contestability. Ultimately, the case illustrates how regulatory coordination across legal domains is essential to uphold fair competition and empower users in the digital economy.

CONCLUSION

This study has examined the central challenge facing data portability frameworks: the disconnect between the theoretical promise of enhancing user autonomy and promoting market competition, and the practical limitations that undermine effective enforcement.

The analysis demonstrates that Article 20 of the GDPR, despite its significance as a user empowerment tool, faces inherent limitations that constrain its effectiveness in addressing market concentration and anti-competitive conduct. The enforcement gap becomes more pronounced when considering that data portability under the GDPR is restricted to personal data actively provided or passively observed by users, excluding inferred or derived data that often holds the greatest commercial value.[80] This narrow scope, combined with privacy-related constraints that can result in fragmented datasets, significantly limits the competitive utility of data transfers.[4] Moreover, even advanced regulatory frameworks like the Digital Markets Act and Data Act face limitations in addressing market competition concerns, as the DMA applies only to designated gatekeepers and the Data Act's effectiveness remains contingent upon the development of interoperability standards and market acceptance of new data sharing obligations.[81]

The Turkish Competition Authority's decision in the *Sahibinden* case marks a pivotal development in the application of data portability, illustrating how competition law can be used to fill enforcement gaps not covered by data protection regimes. Its importance goes beyond the specific market context, presenting a potential model for enforcement that could be considered by European competition authorities.

[80] Krämer, Senellart and de Streel, *Making Data Portability More Effective*, 19-20.
[81] Lazarotto, *Right to Data Portability*, 8, 11.

A crucial factor underlying the TCA's innovative approach was the absence of comprehensive data portability regulation in Turkish law. Unlike the European Union, which has established data portability rights under Article 20 of the GDPR, Turkey's Personal Data Protection Law (KVKK) contains no equivalent provision for general data portability.[82] While Turkey has sector-specific portability regulations, such as the Number Portability Regulation in telecommunications, these are limited in scope and do not extend to digital platform services.[83] This regulatory vacuum meant that traditional data protection remedies were unavailable to address the competition concerns identified in the *Sahibinden* case. The absence of data portability rights under Turkish data protection law forced the TCA to develop competition-based solutions, ultimately leading to more comprehensive and effective remedies than might have been achieved through data protection enforcement alone.

The *Sahibinden* decision highlights how competition law cannot only complement but, in some aspects, go beyond the GDPR by enforcing practical and effective data portability measures. Unlike the GDPR, which depends on user consent and is limited by privacy concerns, the Turkish Competition Authority (TCA) imposed behavioral remedies that required Sahibinden to build the necessary technical infrastructure for seamless data transfers. This obligation was framed as a market correction tool rather than a user-driven right, and it was not constrained by individual consent or third-party privacy issues.

Additionally, the TCA adopted a broader view of data scope compared to Article 20 of the GDPR. While the GDPR limits portability to certain types of personal data and excludes inferred or derived data, the TCA's remedy included a wider range of data, including non-personal and commercially valuable information. This more comprehensive approach helped

[82] Free Privacy Policy, 'Turkey KKVK and the GDPR' (2023) https://www.freeprivacypolicy.com/blog/turkey-kkvk-gdpr/ accessed 15 January 2025.
[83] *Numara Taşınabilirliği Yönetmeliği*, Official Gazette, 2 July 2009, No 27276.

overcome the common issue of fragmented and less useful datasets in GDPR-based data transfers, thereby enhancing the competitive impact of the remedy.

The *Sahibinden* decision introduced several forward-looking features that set it apart from conventional competition law remedies. The Turkish Competition Authority (TCA) required bidirectional data portability, meaning *Sahibinden* had to support not only the export of user data to other platforms but also the import of data from competitors at users' request which is an approach that enhances market symmetry and promotes fairer competition. Also, the decision enforced real-time and continuous data updating, ensuring that any transferred data remains current and usable across different services.[84] This mirrors technical standards in the EU's Digital Markets Act but is applied here within the context of competition enforcement, showing how behavioral remedies can reflect advanced regulatory practices.[85] In addition, the TCA included long-term monitoring obligations, requiring *Sahibinden* to submit annual compliance reports over a three-year period.[86] This element addresses a common criticism of behavioral remedies namely, the risk of long-term non-compliance by introducing sustained oversight.[87]

The Turkish Competition Authority's innovative approach in the *Sahibinden* decision provides several critical lessons for European competition enforcement in addressing data portability concerns and digital market regulation. First, EU authorities must overcome their institutional reluctance toward data portability enforcement. The European Commission's cautious stance contrasts sharply with the TCA's decisive intervention, despite recognizing that "data

[84] TCA, *Sahibinden*, para 817.
[85] Erdem Aktekin, Helin Yüksel and Seda Eliri, 'Preventing Data Portability as Abuse of Dominance: The TCA's Approach in Sahibinden Decision' (Kluwer Competition Law Blog, 17 March 2024) https://competitionlawblog.kluwercompetitionlaw.com/2024/03/17/preventing-data-portability-as-abuse-of-dominance-the-tcas-approach-in-sahibinden-decision/ accessed 10 June 2025.
[86] TCA, *Sahibinden*, para 817.
[87] OECD, *Remedies and Commitments in Abuse Cases*, 25–27.

portability goes to the heart of competition policy," the Commission has maintained a significant enforcement gap, having not yet imposed sanctions based on failures to enable data portability.[88] The *Sahibinden* case demonstrates that competition law constraints need not preclude effective action when authorities clearly link data portability restrictions to specific competition concerns, such as raising switching costs and suppressing multi-homing. Moreover, the existence of GDPR-based portability rights should not preclude competition law intervention, as competition remedies possess superior market-correcting potential compared to individual data protection rights. Additionally, the decision exemplifies the need for adopting sophisticated remedial approaches that address structural market problems through proportionate behavioral remedies targeting specific anti-competitive conduct while preserving platform innovation benefits. The TCA's technical infrastructure requirements demonstrate how authorities can enable competition without dismantling successful business models, mandating bidirectional data portability with real-time updates rather than imposing structural separations. Indeed, enhanced coordination between regulatory domains proves essential, as while the GDPR establishes user rights, competition law provides enforcement mechanisms to ensure meaningful market outcomes.[89] The TCA's success shows that competition law remedies can be effective even absent underlying data protection rights, and may prove more effective than data protection approaches in achieving systematic market-level changes. These lessons collectively point toward a more assertive and technically sophisticated approach to competition enforcement, suggesting that EU authorities should recognize data portability restrictions as clear abuse of dominance when they raise switching costs and suppress multi-homing, with the *Sahibinden* decision can be a roadmap for more ambitious enforcement strategies that match the complexity of contemporary digital markets.

[88] Lynskey, *Aligning data protection rights with competition law remedies?,*4.
[89] Inge Graef, Martin Husovec and Nadezda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19(6) *German Law Journal*, 1388.

BIBLIOGRAPHY

Cases

European Commission, Decision 2007/53/EC of 24 March 2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft) [2007] OJ L32/23

Turkish Competition Authority, *Sahibinden Bilgi Teknolojileri Pazarlama ve Ticaret A.Ş.* Decision (23 August 2023) Case No 23-39/765-263

EU Legislation

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 (General Data Protection Regulation) [2016] OJ L119/1

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data (Data Act) [2023] OJ L354/1

Turkish Legislation

Law No 6698 on the Protection of Personal Data (KVKK), Official Gazette No 29677, 7 April 2016

Number Portability Regulation (Numara Taşınabilirliği Yönetmeliği), Official Gazette, 2 July 2009, No 27276

Official Publications

Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability (WP 242 Rev.01)

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European data economy COM(2017) 9 final, 10 January 2017

Secondary Resources

21 Analytics, 'Citizen's data protection: The EU's GDPR and Türkiye's KVKK' (2025) https://www.21analytics.ch/blog/gdpr-and-kvkk-compared/ accessed 15 January 2025

Aktekin E, Yüksel H and Eliri S, 'Preventing data portability as abuse of dominance: The TCA's approach in Sahibinden decision' (Kluwer Competition Law Blog, 17 March 2024) https://competitionlawblog.kluwercompetitionlaw.com/2024/03/17/preventing-data-portability-as-abuse-of-dominance-the-tcas-approach-in-sahibinden-decision/ accessed 10 June 2025

Chao Y and others, 'Data portability strategies in the EU: Moving beyond individual rights' (SSRN, 2024) https://www.ssrn.com/abstract=4933201 accessed 16 June 2025

Engels B, 'Data portability among online platforms' (2016) 5(2) *Internet Policy Review* https://policyreview.info/articles/analysis/data-portability-among-online-platforms accessed 10 June 2025

Endpoint Protector, 'All you need to know about Turkey's personal data protection law (KVKK)' (2023) https://www.endpointprotector.com/blog/everything-you-need-to-know-about-turkeys-personal-data-protection-law/ accessed 15 January 2025

Free Privacy Policy, 'Turkey KKVK and the GDPR' (2023) https://www.freeprivacypolicy.com/blog/turkey-kkvk-gdpr/ accessed 15 January 2025

Graef I, Husovec M and Purtova N, 'Data portability and data control: Lessons for an emerging concept in EU law' (2018) 19(6) *German Law Journal* 1359

Graef I, Verschakelen J and Valcke P, 'Putting the right to data portability into a competition law perspective' (Social Science Research Network, 2013) https://papers.ssrn.com/abstract=2416537 accessed 10 June 2025

Hey F, *Data interoperability and portability in the DMA: Competition booster or lame duck?* (Ilmenau University of Technology 2024) Ilmenau Economics Discussion Papers No 192

Krämer J, Senellart P and de Streel A, *Making data portability more effective for the digital economy* (CERRE, 2020) https://ssrn.com/abstract=3866495 accessed 30 May 2025

Kranz J and others, 'Data portability' (2023) 65(5) *Business & Information Systems Engineering* 597

Lazarotto B da R, 'The right to data portability: A holistic analysis of GDPR, DMA and the Data Act' (2024) 15(1) *European Journal of Law and Technology* https://ejlt.org/index.php/ejlt/article/view/984 accessed 10 June 2025

Lynskey O, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability' (2017) 42(6) *European Law Review* 793

Maier-Rigaud FP, 'Behavioural versus structural remedies in EU competition law' in Lowe P, Marquis M and Monti G (eds), *European Competition Law Annual 2013: Effective and Legitimate Enforcement of Competition Law* (Hart Publishing 2016)

Mondaq, 'Gap analysis: GDPR vs Turkish personal data protection law (KVKK)' (2018) https://www.mondaq.com/turkey/privacy-protection/724120/gap-analysis-gdpr-vs-turkish-personal-data-protection-law-kvkk accessed 15 January 2025

OECD, *Data portability, interoperability and digital platform competition* (OECD Competition Committee Discussion Paper, 2021) https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf accessed 10 June 2025

Vanberg AD and Ünver MB, 'The right to data portability in the GDPR and EU competition law: Odd couple or dynamic duo?' (2017) 8 *European Journal of Law and Technology*