Administrative Council for Economic Defense

REPORT ON DATA REMEDIES

International Experience with the Application of Data-Related Remedies in Digital Markets: Intersection of Competences and Cooperation between Authorities

CADE
Administrative Council for Economic Defense

DOCUMENT FROM THE ADMINISTRATIVE COUNCIL FOR ECONOMIC DEFENSE (CADE)

Written by

Nicolo Zingales

Consultant at the United Nations Development Programme (UNDP)

Coordinated and proofreading by

Marcus Vinicius Silveira de Sá

Coordinator of the Antitrust Analysis Unit 11 at the Office of the Superintendent General of CADE

Editing and Graphic Designing by

Wandson Lucas Nascimento Siqueira

SUMMARY

(1) INTRODUCTION

This document is the final product of the project "International Experience with the Application of Data-Related Remedies in Digital Markets: Intersection of Competences and Cooperation between Authorities"[1] developed by the Administrative Council for Economic Defense (Cade) with the support of the United Nations Development Programme[2]. The project's central objective is to provide analytical and practical support for the design, implementation, and monitoring of compliance with data-remedies in digital markets, particularly in data-driven digital markets. To this end, this report provides a comprehensive examination of international experience in this field, with special emphasis on the forms of cooperation adopted at the intersection of regulatory competences, namely competition law enforcement and data protection[3].

In 2020, as a co-chair of the ICN Merger Working Group (MWG), the Administrative Council for Economic Defense (CADE) proposed a project within the scope of the 2020-2023 work plan for the biennium 2021-2022. The project consisted of a survey on issues relating to the correlation of data control, market power, and potential competition in merger reviews, and which led to a Report published in 2022[4]. One of the conclusions of the Report concerned the central role that data plays in digital markets. As recognized by several authorities and reports, the possibility of digital firms instantly collecting and processing a considerable amount of data has changed reality drastically, affected competition, and intensified issues related to consumer privacy. However, at the same time, the competitive analysis involving data must consider and differentiate the types of data and their implications for

1 In Portuguese, "a experiência internacional com a aplicação de remédios relacionados a dados (data-remedies) em mercados digitais: interseção de competências e cooperação entre autoridades".

2 Project nº 28/2025 (Process nº 08700.000223/2025-58).

3 CADE, Termo de Referência. Available at: https://cdn.cade.gov.br/Portal/assuntos/noticias/2025/SEI_1503625_Termo_de_Referencia_ajustada.pdf. Accessed 28 August 2025.

4 ICN and CADE. Report on the Control of Data, Market Power and Potential Competition in Merger Reviews (February 2022) Available at <https://cdn.cade.gov.br/Portal/assuntos/noticias/2024/ICN%20MWG%20Report%20Control%20of%20Data%20Market%20Power%20and%20Potential%20Competition%20in%20Merger%20Review%20-%20CADE.pdf>. Accessed 4 December 2025.

market competition, considering data heterogeneity, dimensions, use cases, typology, data access conditions, and levels[5].

In the same vein, CADE's "Working Paper" on Digital Platform Markets[6] ("*Caderno do Cade sobre Mercados de Plataformas Digitais*"), published in 2021, further acknowledges the importance of data as an essential input in the context of digital platforms, particularly insofar as greater data collection and acquisition, in digital environments, are directly associated with increased productivity, market power, and market share. Personal data therefore hold incalculable economic value, which in turn attracts significant market interest. At the same time, and especially in light of their intrinsic connection to privacy, several jurisdictions now recognize the right to data protection—sometimes even as a fundamental right, as is the case in Brazil[7].

Also, in 2024, CADE published the Second Report by the Working Group on the Digital Economy, entitled "BRICS in the digital economy: competition policy in practice"[8]. The report was aimed to discuss some principles of the antitrust assessment of markets characterized by a significant digital component. In doing so, it outlined issues concerning data power, conduct involving data collection and use and remedies of access, separation and sharing of data. It also recognized that remedies in digital markets may prescribe conduct that falls within the competence of a non-antitrust regulator, in which case the respective regulatory agency may play a significant role in the monitoring phase (in addition to participating in the design phase). It called attention to the fact that coordination between different agencies may generate

5 ICN and CADE. Report on the Control of Data, Market Power and Potential Competition in Merger Reviews (February 2022) Available at <https://cdn.cade.gov.br/Portal/assuntos/noticias/2024/ICN%20MWG%20Report%20Control%20of%20Data%20Market%20Power%20and%20Potential%20Competition%20in%20Merger%20Review%20-%20CADE.pdf>. Accessed 4 December 2025, para. 248.

6 CADE. Caderno de plataformas digitais. Available at: <https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/plataformas-digitais.pdf>. Accessed 4 December 2025, p. 11-12.

7 See, for instance: DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. Available at: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Accessed 4 December 2025.

8 CADE, BRICS in the digital economy: competition policy in practice (January 2024). Available at <https://cdn.cade.gov.br/Portal/assuntos/noticias/2024/BRICS%20Digital%20Economy.pdf>. Accessed 4 December 2025.

tensions, especially when the law holds that the action of the antitrust agency is pre-empted where a regulatory agency has authority to regulate competition[9]; and recommended the stipulation of dedicated cooperation agreements to enhance the effectiveness of interinstitutional cooperation in remedy design and implementation[10].

More than sharing a common objective, competition law and data protection exhibit significant complementarities, which must be duly considered in order to ensure the effective fulfillment of their respective and specific mandates[11]. In acknowledgment of this evolving institutional landscape and the growing interdependence between the two regulatory spheres, the Brazilian Competition Authority has already taken proactive steps to strengthen dialogue and coordination with the Brazilian National Data Protection Agency (ANPD). To this end, a Technical Cooperation Agreement (TCA)[12] was executed to establish structured mechanisms for mutual support and the development of joint and coordinated initiatives in matters that lie at the intersection of competition enforcement and data protection. This reflects CADE's ongoing commitment to deepening its institutional expertise and fostering sustained cooperation in addressing the complex challenges posed by data-driven digital markets.

Against this backdrop, the present Report builds upon CADE's broader efforts to map international best practices concerning the interface between data protection and competition law[13]. In light of the

9 CADE, BRICS in the digital economy: competition policy in practice (January 2024). Available at <https://cdn.cade.gov.br/Portal/assuntos/noticias/2024/BRICS%20Digital%20Economy.pdf>. Accessed 4 December 2025, p. 170. See also KWOKA, J., & MOSS, D. (2012). Behavioral Merger Remedies: Evaluation and Implications for Antitrust Enforcement. The Antitrust Bulletin, 57(4), 979-1011.

10 CADE, BRICS in the digital economy: competition policy in practice (January 2024). Available at <https://cdn.cade.gov.br/Portal/assuntos/noticias/2024/BRICS%20Digital%20Economy.pdf>. Accessed 4 December 2025, p. 171. See also ZINGALES, N. (2018). Data Protection Considerations in EU Competition Law: Funnel or Straitjacket for Innovation? In P. NIHOUL, & P. V. CLEYNENBREUGEL, The Role of Innovation in Competition Analysis (pp. 79-130). Edward Elgar. Available at doi: http://dx.doi.org/10.2139/ssrn.3158008.

11 See, for instance, SILVEIRA DE SÁ, Marcus V. 'Integrando proteção de dados e defesa da concorrência: rediscussão do papel do direito antitruste e seu ferramental clássico na economia digital movida a dados'. Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), Brasília, Distrito Federal, 2023.

12 Cooperation Agreement nº 51/2021 (CADE/ANPD). Available at <https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf>. Accessed 4 December 2025.

13 See, for instance, Departamento de Estudos Econômicos. Documento de Trabalho N°

increasing recognition of the competitive significance of data – and of the corresponding need for coordination among regulatory authorities – CADE undertook an in-depth study of arrangements in place in different jurisdictions for the adoption of data-related remedies. As a result of that study, this Report was drafted. It therefore serves not only to enable the Authority to assume a more active role in global discussions on data protection and competition enforcement, but also in ensuring that it maintains a leading position among its peers while proactively anticipating the challenges that are likely to be brought before the Council in the near future[14].

002/2021 Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados. Available at <https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2021/Documento%20de%20Trabalho%20-%20Benchmarking-internacional-Defesa-da-Concorrecia-e-Proteacao-de-dados.pdf>. Accessed 28 August 2025.

14 See CADE, Termo de Referência. Available at: <https://cdn.cade.gov.br/Portal/assuntos/noticias/2025/SEI_1503625_Termo_de_Referencia_ajustada.pdf>. Accessed 28 August 2025.

(2) METHODOLOGY

The present research was conducted on the basis of two complementary methodologies: (i) the circulation of a structured questionnaire to foreign competition authorities and (ii) desk research.

First, the questionnaire was drafted in English and sent, on May 2025, to 119 authorities across different jurisdictions, with the purpose of mapping: (i) the legal framework for data protection in each jurisdiction and the potential competence of competition authorities to impose data-related remedies; (ii) formal and informal cooperation with data protection authorities (Data Protection Authorities – DPAs); and (iii) the existence and use of data remedies in cases involving anticompetitive conduct and merger control proceedings. In total, 20 jurisdictions submitted responses to the questionnaire[15].

It should be noticed that 2 (two) authorities – those of Germany and the United Kingdom – opted not to respond to the specific questions contained in the questionnaire, instead providing links to publicly available information describing their general institutional practices. Also, besides those 20 responses, the European Commission provided an informal response through a virtual meeting followed by an explanatory email. The information received were systematized and constitute the empirical basis of this Report.

In addition to that, relevant information was gathered through the "Webinar on Data-Related Remedies" organized by the Administrative Council for Economic Defense (CADE) within the framework of the International Competition Network (ICN) as a co-chair of the Unilateral Conducts Working Group (UCWG). The discussions and contributions presented during the event provided further insights and comparative perspectives on the design and implementation of data-related remedies.

Finally, to complete the material initially collected through questionnaire and webinar, a desk research was conducted, consisting of documentary and bibliographical research based on the analysis of

15 Argentina, Canada, Costa Rica, Croatia, Czech Republic, Ecuador, Georgia, Greece, Hungary, Italy, Japan, Kenya, Latvia, Mexico, Paraguay, Peru, Philippines, Switzerland, United Kingdom, and Zambia.

primary and secondary sources, including legislation, administrative decisions, institutional reports, academic publications, and publicly available official documents. This complementary work aimed to further explore and contextualize the information obtained through the questionnaire and fill any relevant gaps.

(3) ABOUT THIS REPORT

This Report aims to facilitate the mapping of international best practices and of existing discussions on data remedies. To that end, it outlines different types of data remedies on the basis of their main characteristics and discusses the challenges for their implementation.

At the outset, definitions should be provided regarding the concepts of "data" and "data remedies".

While the term "data" is often used in a non-technical sense in everyday parlance, a clarification is necessary in order to delimit the scope of the present inquiry. For purposes of this report, we define it as "any digital representation of acts, facts or information and any compilation of such acts, facts or information", following a definition given by the European institutions in its Data Governance Act[16]. It is worth noting that this includes both personal data, (*i.e.* those that are liable to make an individual identified or identifiable[17]), and non-personal data, and that the former category brings more substantive operational challenges because it attracts the application of privacy and data protection law.

"Data remedies" is used here to refer to remedies imposed to address competition issues that relate to the collection, storage, formatting, sharing and use of data. A useful taxonomy of data remedies has been provided by the Competition and Markets Authority (CMA) as part of their Market Study on Online Platforms and Digital Advertising[18], pointing out to five categories: (1) Increasing consumer control over the use of data; (2) Mandating Interoperability; (3) Mandating third-party access to data; (4) Mandating data separation/data silos/ restrictions on certain uses or sharing of data; (5) Allowing regulatory scrutiny and audit.

16 Art. 2 (1) of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1, OJ L 152, 3.6.2022, pp. 1–44.

17 In Brazil, the concept of personal data is defined in Law No. 13,709/2018, known as the General Data Protection Law (LGPD), specifically in Article 5, I, as follow: "Article 5. For purposes of this Law, the following definitions shall apply: I – personal data: information regarding an identified or identifiable natural person;"

18 CMA. Market Study on Online Platforms and Digital Advertising (July 2020), Annex T. Available at <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>. Accessed 4 December 2025.

For purposes of this Report, we expand this typology to ten categories, to reflect distinctions between some of the categories of remedies within the typologies identified by the CMA. In particular, we consider:

(i) Data portability: permitting the download and the voluntary transfer of data to other businesses upon consumer request[19];

(ii) Data interoperability: enabling two or more systems or components to exchange information and to use the information that has been exchanged[20];

(iii) Data segregation: the separation of datasets in order to prevent their combination[21];

(iv) Data sharing: mandating the disclosure of data to a third party[22];

(v) Data control enhancement: increasing consumer control over the use of data, for instance by requiring additional consent or notification and opt-out possibilities[23];

(vi) Application of PETs: Improving privacy protections to one or more datasets through use of Privacy Enhancing Technologies (PETs)[24];

19 For instance, according to article 20 of Regulation (EU) 2016/679, the right to data portability allows individuals to "receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".

20 See, for instance, FCC, "Interoperability". Available at <https://www.fcc.gov/general/interoperability>. Accessed 4 December 2025. See also GULATI-GILBERT, S., SEAMANS, R. Data portability and interoperability: A primer on two policy tools for regulation of digitized industries (Brookings, May 2023). Available at <https://www.brookings.edu/articles/data-portability-and-interoperability-a-primer-on-two--policy-tools-for-regulation-of-digitized-industries-2/>. Accessed 4 December 2025.

21 See, for instance, Privacy Engine. "Data Segregation". Available at <https://www.privacyengine.io/resources/glossary/data-segregation/>. Accessed 4 December 2025.

22 See, for instance, ICO. "Data sharing covered by the Code". Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code--of-practice/data-sharing-covered-by-the-code/. Accessed 4 December 2025.

23 For instance, the CMA cites requiring consent for use of data, facilitating informed choice, facilitating data mobility. CMA, Market Study on Online Platforms and Digital Advertising (July 2020), Annex T, T5.

24 According to the European Union Agency for Cybersecurity (ENISA), PETs are "Software and hardware solutions, i.e. systems encompassing technical processes, methods or

(vii) Data transparency: granting access to datasets for the purposes of regulatory scrutiny and audit[25];

(viii) Data use prohibition: prohibition to use datasets with a specific purpose or effect[26];

(ix) Data anonymization: obligation to the process of turning personal data into anonymous information so that a person is no longer identifiable[27];

(x) Data disgorgement: obligation to eliminate one or more datasets[28].

knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons". Examples are: Differential Privacy; Synthetic Data; Homomorphic encryption; Zero-Knowledge Proof; Trusted Execution Environments; Secure multiparty computation; Federated Learning. See ICO. "What PETs are there?". Available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/what-pets-are-there/.> Accessed 4 December 2025.

25 For instance, the CMA cites transparency of ad tech fees and regulatory scrutiny of Auctions. CMA, Market Study on Online Platforms and Digital Advertising (July 2020), Annex T, T5.

26 For instance, this remedy was accepted by the European Commission as a condition to clear the acquisition of Fibit by Google, whereby Google would be prevented from using Fitbit health and wellness data would not be used for Google ads. See EUROPEAN COMMISSION. *"Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions" (Press Release, 16 December 2020).* Available at <https://ec.europa.eu/commission/presscorner/detail/it/ip_20_2484>. Accessed 4 December 2025.

27 See, for instance, ICO. "Introduction to anonymization". Available at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/introduction-to-anonymisation/>. Accessed 30 March 2026.

28 FEDERMAN, H. "Tainted fruit: Disgorgement of data from the FTC and beyond" (27 April 2021). Available at https://iapp.org/news/a/tainted-fruit-disgorgement-of-data-from-the--ftc-and-beyond.

(4) CHARACTERISTICS OF DATA

Several legal and economic reports suggest that data is an economic asset with its own peculiarities: most notably, in addition to having value in itself[29], which means that it can be traded in consideration for goods and services, it is also an infrastructural resource[30]: this means that it is non-rivalrous, instrumental as an input for the production of goods and services (although the relationship of input to output is not always clear or linear), and of general purpose. The latter characteristic is also linked to its nature of an inchoate resource, generally necessitating some cleaning, refinement and organization to be used as a structured source of knowledge[31]. Furthermore, data can be individualizing, meaning that it can directly or indirectly relate to an individual, and thereby enable personalized offering.

The above suggests that, from a competitive standpoint, one can conceive remedies relating to the use of personal data for at least two different purposes: first, as an input for *building* new products and services, including, for instance, the training of algorithms; and second, as an asset with personalization capacity that can be exploited to *offer* personalized products and services[32]. While the former exhibits some tensions with data protection law, as it points to the need to open up data

29 See, for instance, OECD, 'Data-driven Innovation: Big Data for Growth and Well-being' OECD Publishing:2015; The Economist. The World's Most Valuable Resource is Data; <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> and <https://assets.publishing.service.gov.uk/media/5b62c26aed915d4b4a12ae42/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf>. Accessed 30 March 2026.

30 Bret Frischmann, *Infrastructure: The Social Value of Shared Resources* (Oxford University Press, 2012), *apud* Thomas Thombal, *Imposing Data Sharing Among Private Actors: A Tale of Evolving Balances* (Wolters Kluwer, 2022) 53. Raul Castro Fernandez. 2025. What is the Value of Data? A Theory and Systematization. ACM / IMS J. Data Sci. 2, 1, Article 3 (March 2025), 25 pages. <https://doi.org/10.1145/3728476>. Accessed 30 March 2026.

31 Robert Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Sage, 2014) 6.

32 This is directly related to *behavioral advertising*. About the topic, See, e.g., Dissenting Statement of Commissioner Rohit Chopra, *In re Google LLC and YouTube, LLC*, Commission File No. 1723083 (Sept. 4, 2019), *in verbis*: "Behavioral advertising, unlike contextual advertising, is about targeting each individual – a demographic of one. […] Google is able to glean more and more insights about their personal lives. Google then monetizes these insights by using them to psychologically profile each user and predict in real time what content will be most engaging and which ads will be most persuasive". See also ICN, 'Competition law enforcement at the intersection between competition and privacy: agency considerations' (2024), p. 13: "Nor is the focus necessarily providing individuals with more relevant ads; instead, they may use the personal data to better predict and manipulate consumer behavior."

to third parties, the latter illustrates the synergy between competition and data protection law, to the extent that it results in preventing undue use of the personalizing capacity of data to obtain a competitive advantage.

One of the first document discussing the interaction between these two disciplines is the Joint Study of the *Bundeskartellamt* and the French *Autorité de la Concurrence* entitled 'Competition Law and Data'[33]. Starting from the well-known distinction between volunteered, observed, and inferred data[34], the Study ends up attributing more relevance to two macro-categories, namely first-party data (datasets created by the same firm) and third-party data (data that has been transferred from other data collectors). According to the Study, those who have third-party data obtain larger and more diverse datasets, with lower fixed costs and higher variable costs than those who merely rely on first-party data. Nevertheless, despite the potential value and availability of third-party data, it might still be difficult for new entrants to match the quality of first-party data sitting in the hands of incumbents. This suggests that data sharing may be necessary to create a level playing field, when the absence of this raises competitive issues.

The second type of manifestation of data power relates to the ability to use personal data of individuals to make targeted offers. This is another contentious area, especially due to the potential synergies between competition and data protection law, which impose limits on how personal data can be used as an input in those offers, and consumer protection law, which imposes limits relating to their transparency. Therefore, a key question here from a competition law standpoint is the extent to which it should take into account the existence of a violation of legislation in other areas.

On one hand, supporters of limited antitrust intervention argue that competition authorities should not replicate or replace the job of data

33 Bundeskartellamt and Autorité de la Concurrence, *Competition Law and Data* (2016). Available at <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2> Accessed 15 February 2023.

34 Organization for Economic Co-operation and Development (OECD), *Data-Driven Innovation: Big Data for Growth and Well-Being Paris*(2015), available at <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 February 2023.

protection and consumer protection authorities, arguing that data privacy and consumer protection considerations are not within the purview of antitrust[35]. Under this view, competition authorities should refrain from assessing those violations so as to respect the institutional division of competences, in particular because different regimes protect against different kinds of harm[36]. On the other hand, it is argued that an infringement of those two laws can be used to strengthen one's market position and, therefore, could be cognizable under competition law. This is considered appropriate because all these areas share the goal of promoting consumer welfare[37]; and specifically, for data privacy, because it is a fundamental right that as such must be recognized, protected and promoted by other regulators[38]. An intermediate position is also possible, holding that data protection violations should be considered only to the extent that data protection is a relevant dimension of competition in that market, for instance from the perspective of product quality[39].

Regardless of the view taken, this intersection points to the need for cross-institutional collaboration, which has been initiated in a number of jurisdictions between competition, consumer protection and data protection authorities: examples are the Digital Clearinghouse initiative in the European Union[40]; the Digital Regulation Cooperation Forum in the United Kingdom[41]; The Digital Regulation Cooperation Platform (SDT) in

35 James C. Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity' (2013) 20 *Geo. Mason l. Rev*. 1129, 1146; Maureen K. Ohlhausen and Alexander P. Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 Antitrust L.J. 121, 138- 143.

36 Ibid.

37 Albertina Albors-Llorens, ´Competition and Consumer Law in the European Union: Evolution and Convergence´ (2014) 33(1) *Yearbook of European Law*, 163; Samson Y. Esayas, ´Competition in (Data) Privacy: 'Zero'-Price Markets, Market Power, and the Role of Competition Law´ (2018) 8(3) *International Data Privacy Law*, 181.

38 Inge Graef, *EU Competition Law, Data Protection and Online Platforms. Data as Essential Facility* (International Competition Law Series, Vol. 68, Wolters Kluwer, 2016), 256; Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54(1) *Common Market Law Review*, 11; Nicolo Zingales, 'Data Protection Considerations in EU Competition Law: Funnel or Straightjacket for Innovation?' in P. Nihoul and P. Van Cleynenbreugel (eds.), *The Role of Innovation in Competition Analysis*(Edward Elgar, 2018), 79.

39 Erika Douglas, ´The New Antitrust/Data Privacy Law Interface´ (2021) 647 *The Yale Law Journal Forum*, 1.

40 See Digital Clearing House', available at <https://www.digitalclearinghouse.org>. Accessed 30 March 2026.

41 Competition & Markets Authority (CMA), Information Commissioner's Office (ICO) and

the Netherlands[42]; the Digital Regulators Group, in Ireland[43]; the Digital Cluster Bonn, in Germany[44]; and the national network for coordination of the regulation of digital services, in France[45]. These collaborative efforts can stimulate synergistic solutions between different regulators, with a view to adopting data remedies that may not merely restore competition but also promote more privacy-friendly alternatives, preserving or improving conditions for data privacy and the exercise of data subject rights under the applicable data protection legislation.

Ofcom, Digital Regulation Cooperation Forum, available at <https://www.ofcom.org.uk/__data/assets/pdf_file/0021/192243/drcf-launch-document.pdf> Accessed 15 February 2023.

42 See <https://www.acm.nl/en/about-acm/organization/cooperation/national-cooperation>. Accessed 30 March 2026.

43 See <https://www.comreg.ie/about/other-regulators/>. Accessed 30 March 2026.

44 See <https://www.digitalclusterbonn.de/DCB/PM1.pdf?__blob=publicationFile&v=4>. Accessed 30 March 2026.

45 See <https://www.legifrance.gouv.fr/download/pdf?id=7LmXEZdnLi7eCA44AfI3DzMbWZAFbcTslqsHhe5AbcM=>. Accessed 30 March 2026.

(5) MAPPING OF RESPONSES TO THE QUESTIONNAIRE – DATA PROTECTION AUTHORITIES AND COOPERATION MECHANISMS

Out of 20 responses received, 19 jurisdictions reported having an independent data protection authority, without subordination to any coordinating body or other public authority. The exception is **Paraguay**, where the protection of personal credit data falls under the jurisdiction of the Central Bank of Paraguay (BCP) and the Secretariat for Consumer and User Protection (SEDECO), pursuant to National Law No. 6534/2020.

Peru reported having an independent authority, though it admitted that it hierarchically depends on the Vice-Ministerial Office of Justice of the Ministry of Justice and Human Rights. As for **Ecuador**, the competition authority (Superintendence of Economic Competition of Ecuador) affirmed that it has (some) competence in matters of data privacy. This is based on Article 48 of the Organic Law on Regulation and Control of Market Power (LORCPM), which grants it the power to access, consult, archive, process, and use any data relevant to its functions, while respecting the constitutional right to information protection.

Specifically concerning cooperation between data protection and competition authorities, out of the 20 responses received, only 5 (**Canada, Philippines, Greece, Hungary, and Czech Republic**) reported having formal mechanisms of cooperation between their independent authorities. Additionally, the competition authorities of 3 jurisdictions (**Switzerland, Ecuador and Latvia**) pointed to the fact that the law establishes a formal duty of cooperation, and in 2 cases (**Ecuador and Latvia**) agreements have been made between several competent authorities relating to the implementation of specific legislations.

Among the formal cooperation mechanisms, the following were mentioned: (i) Memorandum of Understanding; (ii) Cooperation forums; and (iii) Cooperation agreements.

In the **Philippines**, the Memorandum of Agreement (MOA) signed between the Competition Commission and the Privacy Commission in

2022 created formal communication and notification channels between authorities for enforcement support and access to information[46]. The MoA establishes the duties to notify each other in matters touching on each other's competence, excluding, however, matters obtained through compulsory process. It also establishes the duty to respond to requests of access to information by the other party in 6 business days and prescribes an amicable settlement process for any disputes that may arise. Finally, it encourages authorities to do joint capacity building, joint task forces, and to coordinate for the adoption of public statements.

In **Greece**, the Memorandum of Cooperation (MOC), also signed in 2022 by the authorities, enables information exchange, mutual assistance (including in investigations), the creation of working groups for the development of guidelines and studies, as well as the organization of seminars and workshops for internal training and for informing economic agents. The MOC also established a Joint Coordination Committee to implement the memorandum, with or without the participation of third-party stakeholders.

In the **Czech Republic**, a Memorandum of Cooperation was also signed between the two authorities in 2025, planning the creation of a joint working group and the publication of joint guidance for the general public on the relationship between the two authorities. **Hungary** also reported the existence of a specific agreement between its independent authorities, signed in 2015 and replaced in 2020, which provides for mechanisms such as regular consultations, mutual notifications, and information exchanges in specific cases, pre-legislative coordination, joint communication actions and events, as well as the obligation to designate contact points between the authorities.

Paraguay, exceptionally, stated that it has agreements in place between the BCP, SEDECO, and its competition authority, but that such agreements are generic and do not specifically address the protection of personal credit data.

46 See <https://www.phcc.gov.ph/storage/pdf-resources/1678087136_2022-02-09-MO-A-National-Privacy-Commission.pdf>. Accessed 30 March 2026.

Of all the responding authorities, although many do not have formal mechanisms, only three (**Mexico, Paraguay, and Peru**) did not report any specific "informal" cooperation mechanism used to facilitate and promote dialogue between the two independent authorities. Among the main dialogue and cooperation mechanisms mentioned, the following stand out: (1) joint sector inquiry (**Italy**); (2) information sharing through requests or notifications, communication (whether by telephone or otherwise), and meetings (remote or in person) (**Argentina, Canada, Costa Rica, Croatia, Italy, Japan, Latvia, Kenya, Zambia**); and (3) training and capacity-building activities for staff (**Kenya, Zambia**).

Ecuador presents a peculiar scenario in which, although no specific informal cooperation mechanisms were identified, both the competition authority and the data protection authority belong to the Transparency and Social Control Branch (FTCS), which allows for fluid communication between them. In addition, national law allows the Ecuadorian competition authority to enter into cooperation agreements with other public bodies, and to request information from such entities.

(6) THE INTER-INSTITUTIONAL CONUNDRUM: HOW TO FACILITATE COOPERATION

Cooperation amongst authorities tasked with overlapping or parallel competences is a key challenge for regulation in an interconnected world, and the intersection of competition and data protection law offers a vivid illustration of this phenomenon.

To tackle this topic, one can learn from the protocols of cooperation developed by the European Union, the only jurisdiction that, so far, has specifically ruled on it.

According to the **European Court of Justice** (CJEU)'s 2023 decision in **Case C-252/21**, a competition authority may consider data protection rules when assessing data-related cases under antitrust law[47]. In CJEU's words, "the compliance or non-compliance of that conduct with the provisions of the GDPR may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers"[48].

Indeed, the Court endorsed the argument made by the Commission that access and the ability to process personal data have become a significant parameter of competition between undertakings in the digital economy, and thus, excluding data protection rules from the analysis of competition authorities would be liable to undermine the effectiveness of competition law within the European Union[49]. However, in view of the different objectives pursued by competition law and data protection, where a national competition authority identifies an infringement of data protection in the context of an investigation, it cannot replace the supervisory authorities. This is because that national competition

47 For further information, see <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2024/OECD_2024_intersection_between_competiton.pdf?__blob=publicationFile&v=3>. Accessed 30 March 2026.

48 Para. 49.

49 Para 51.

authority neither monitors nor enforces the application of that regulation for the purpose referred to in Article 51(1) of the GDPR, namely in order to protect the fundamental rights and freedoms of natural persons in relation to processing or to facilitate the free flow of personal data within the European Union.

Therefore, the CJEU's decision determined that "where a national competition authority considers it necessary to rule, in the context of a decision on an abuse of a dominant position, on the compliance or non-compliance with data protection law of the processing of personal data by the undertaking in question, the respective authorities *must cooperate* with each other in order to ensure the consistency of application of that regulation[50]". Specifically, in view of the duty of sincere cooperation[51], the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms[52]. Where it has doubts as to the scope of such a decision, where those terms or similar terms are, simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with the GDPR, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment[53]. Only upon receiving a response, or in the absence of any objection on their part or of any reply within a reasonable time, may the national competition authority continue its own investigation[54], as per decided.

While this case provides an important path for cooperation in specific cases, it is silent on the procedures and the governance mechanisms that authorities define to facilitate such cooperation. Judging from the cases

50 Para 52.

51 The duty of sincere cooperation requires the Union and the Member States to assist each other, in full mutual respect, in carrying out tasks which flow from the Treaties. See Art. 4(3) of the Treaty on the European Union.

52 Para 57.

53 Para 57-58.

54 Para 59.

involving data remedies so far, it seems that such cooperation often takes place on an *ad hoc* basis (without a specific legal obligation to do so), sometimes informally (without the submission of written requests) and without predefined channels.

Besides cooperation once proceedings have initiated, there are broader sets of circumstances that may require dialogue and collaboration between authorities[55], such as interdisciplinary discussions to shed light on market dynamics, and requests for explanation about legal and technical concepts that fall within another agency's mandate. Depending on the situation, there may be different coordination mechanisms at play: from a merely formalist duty to consult, without corresponding duty to respond, to more demanding procedure that require public response or provide veto power to another agency, or more elaborate duties that involve repeated interactions and even the adoption of joint guidelines or regulations, for example.

For this reason, some suggest the creation of a forum to facilitate discussion between regulators, as done by the European Data Protection Supervisor in 2016 with the establishment of the Digital Clearinghouse[56]. Among all their initiatives, for the purpose of this Report, one must highlight the launch of the Concept Note "Towards a Digital Clearing House 2.0"[57], that reveals a more ambitious plan to solve some of the practical challenges for effective cooperation while recognizing obstacles such as (i) a lack of resources of competent authorities; (ii) a lack of awareness/expertise in other legal fields or lack of knowledge about other enforcement activities; (iii) a lack of willingness to engage beyond one's own regulatory remit, due to a tendency to protect one's own competence ('regulatory tribalism'); and (iv) a lack of ability to lawfully share information and evidence concerning pending investigations. In addition, the Concept Note mentions factors such as the (i) lack of

55 FREEMAN, Jody; ROSSI, Jim. Agency Coordination in Shared Regulatory Space. Harvard Law Review, Cambridge, v. 125, n. 5, p. 1131-1211, 2012.

56 EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data. See <https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf>. Accessed 30 March 2026.

57 EDPS, Concept Note: Towards a Digital Clearinghouse 2.0 (15 January 2015): <https://www.edps.europa.eu/system/files/2025-01/towards_a_digital_clearinghouse_2_0_january_2025_en_0.pdf>. Accessed 30 March 2026.

independence, (ii) the fragmentation of cooperation on a per-instrument basis, (iii) the general inability to invite to official meetings authorities other than competent authorities, and (iv) the absence of legal provisions explicitly mentioning the need for cooperation.

Ensuring effective inter-institutional cooperation, therefore, is not an easy task, but authorities must rise to the challenge and face them in order to be able to appropriately address ever more complex concerns regarding this intersection between competition law and data protection.

(7) SPECIFIC TYPES OF REMEDIES

In this section, we review the characteristics of specific types of data remedies, highlighting promises and challenges in their implementation. We proceed in the following order: first, we define the concept and mention important details regarding its scope and implementation. Secondly, we provide examples (if any) that illustrate how the remedy was applied in a specific case. Finally, we conclude with some reflections on lessons learned and possible ways forward.

(i) Data Portability

Definition

Data portability may be the leading example of alignment between competition and data protection objectives[58]. This alignment can be achieved through remedies imposed by a competition authority, but it is also promoted by legislation.

The primary legislative reference (if anything, for being the first one in its kind) is article 20 of the EU General Data Protection Regulation (GDPR)[59], which allows data subjects to receive their personal data in a structured, commonly used and machine-readable format and to obtain the transmission of those data (where technically feasible) to another controller without hindrance from the controller to which the data have

58 See Diker Vanberg, A. & , Ünver, MB., "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", in European Journal of Law and Technology, Vol 8, No 1, 2017. Lynskey, O. (2017). Aligning data protection rights with competition law remedies? The GDPR right to data portability. European Law Review, 42(6), 793 - 814.

59 "Art. 20. Right to data portability. 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others." See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. OJ L 119, 4.5.2016.

been provided. This provision is consistent with EU data protection law's dual objective of protecting fundamental rights of individuals whose data are processed and encouraging the free movement of data within the internal market[60]. Considering article 20, in particular, while portability can be seen as an extension of control over personal data which enables a data subject to maintain the most effective protection throughout the data lifecycle, the free movement objective supports legislation enabling individuals to overcome the lock-in effect[61] generated by the accumulation of their personal information in data silos[62].

That said, the application of this right under EU data protection law is conditioned upon several requirements, which restrict its scope of application: the first one relates to the legal basis for the processing of the data in the first place, as it only applies to processing that is based on the legal ground of consent of the data subject or for a necessity to enter into or perform a contract with the data subject. Secondly, the data subject to the request had been provided by the individual, which according to the Opinion on Data Portability[63] issued by the Article 29 Working Party ("A29 WP", EU's former advisory body on data protection) is met not only with voluntarily provided data, but also with data observed from the activities of the user[64]. The category that is left out is thus the one of "derived" or "inferred" data, which is generated by the controller through subsequent analysis using the observed or directly provided data as input. And since derived or inferred data may be an important source of a platform's competitive advantage or market power[65], excluding it could significantly limit the effectiveness

60 O. Lynskey, 'From Market- Making Tool to Fundamental Right. The Role of the Court of Justice in Data Protection's Identity Crisis', in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet *European Data Protection: Coming of Age* (Springer, Berlin 2013) 59-84, 63.

61 Lock-in is a problem that arises when consumers must incur specific setup costs to adopt a new product. See e.g. Nancy Gallini and Larry Karp, Sales and Consumer Lock-in Economica New Series, Vol. 56, No. 223 (Aug. 1989), pp. 279-294. See also Jiawei Zhang. The Paradox of Data Portability and Lock-in Effects. Harvard Journal of Law & Technology Volume 36, Number 2 Spring 2023

62 Orla Lynskey, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability' (2017) 6 European Law Journal, 793-814.

63 Article 29 Working Party, '*Guidelines on the Right to Data Portability'* (13 December 2016), 16/EN WP 242, 11.

64 Article 29 Working Party, '*Guidelines on the Right to Data Portability'* (13 December 2016), 16/EN WP 242, 11.

65 See e.g. Peter Swire, The Portability and Other Required Transfers Impact Assessment

of portability as a competition remedy. Furthermore, even for covered data, the interpretation of the proper scope is difficult: it is not always easy to determine if data is "raw" (and portable) or "inferred" (and non-portable), which may hinder effective implementation.

There are also negative conditions for the application of the right to data portability of article 20 of the GDPR, requiring that (1) it does not concern processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (2) its exercise is of no prejudice to the right to erasure provided by article 17 GDPR; and (3) it does not adversely affect the rights and freedoms of others.

Of these negative conditions, the third may open up to balancing with potentially conflicting values, due to the fact that personal data that is subject to the request may simultaneously involve personal data of third parties ("networked data"). About this topic, the Article 29 Working Party gives the example of a directory of data subject's contacts, suggesting that the data controller can only accept to process such requests to the extent that there is a valid legal basis, for example a legitimate interest, which could be met if the new data controller was to provide a service allowing data subjects to process their personal data for purely personal or household activities[66]. This interpretation, which presumes that the original data controller obtains specific and sufficiently reassuring information about the subsequent use of the received data, seeks to protect the data protection of third party data subject, whose fundamental rights could otherwise be seriously impacted by an unscrupulous application of the right to data portability. At the same time, the reference to "private or household uses" can also be seen as a safeguard against possible effects on competition derived from a strategic use of the right to data portability in order to gather commercial value from third-party data.

(PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations, 6 GEO. L. TECH. REV. 57, 115–18 (2022).

66 The Article 29 Working Party gives the example of a directory of data subject's contacts, suggesting that the data controller can only accept to process such requests to the extent that there is a valid legal basis, for example a legitimate interest, which could be met if the new data controller was to provide a service allowing the data subject to process his personal data for purely personal or household activities. *Id.*, 12.

Aside from the specific instance of networked data, other concrete possibilities of conflict may arise between the right to data portability and the rights or freedom of third parties. The A29 WP Guidelines merely mention one of these possibilities, specifically the tension with intellectual property or trade secrets, recalling one of the Recitals of the GDPR[67] according to which "the result of those considerations should not be a refusal to provide *all* information to the data subject". This is certainly not an exhaustive indication of how such conflicts should be resolved, but provides a hint that one-sided solutions (*e.g.,* absolute refusal in deference to trade secrets) would not be acceptable. It can thus be expected that a data controller takes reasonable measures to provide as much information requested as possible by decontextualizing personal data from proprietary algorithms or trade secrets[68].

This arguably won't be an issue as far as *provided* data is concerned, since such data reveals little about the inner workings of the systems used to store and analyze them. On the other hand, intellectual property and trade secrets may present some challenges when it comes to *observed* data, which can be difficult to disentangle from the categories designed by the controller to process the data inputs. Even in cases where de-contextualization is not feasible, however, the fact that data is transferred onto the data subject or a different data controller does not imply that the underlying intellectual property will be violated. That understanding[69] appears reflected in the statement by the Article 29 WP Guidelines that "a potential business risk cannot, in and of itself, serve as the basis for a refusal to answer the portability request". Yet it may raise a question of what threshold ought to be for substantiation of such a risk, such that they entitle a data controller-right holder to prevent future infringements of IP rights in the context of data portability requests. This is a matter largely left open to future guidelines (by the EU Data Protection Board) and legislation, with Recital 73 of the GDPR offering

67 Recital 63 GDPR, in the context of the right of access.

68 Gianclaudio Maglieri, 'Trade Secrets v Personal Data: a possible solution for balancing rights' (2016) International Data Privacy Law 6 (2), 102-116.

69 See Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (December 15, 2017). TILEC Discussion Paper No. 2017-041; Tilburg Law School Research Paper No. 2017/22. Available at SSRN: https://ssrn.com/abstract=3071875 or http://dx.doi.org/10.2139/ssrn.3071875. Accessed 10 July 2018.

examples and stressing the need for any restrictions to data portability to be in compliance with the EU Charter of Fundamental Rights[70] and the European Convention of Human Rights[71].

This overview shows one way in which the right to data portability is regulated. The concept of data portability, introduced in EU data protection law in 2016, has been incorporated in the data protection laws of other jurisdictions. For instance, the Brazilian data protection law, introduced in 2018, establishes in its article 19 (3) a right to obtain an electronic copy of personal data in a form that enables its further processing (indirect or intermediated portability), whenever the original processing was grounded on the legal basis of consent or contract; and includes in its article 18 a right to have personal data transferred to another controller (direct portability).

Other jurisdictions cover more details on the implementation of this right: for instance, Singapore explicitly excludes from its scope derived data[72] and prescribes the preservation of a complete and accurate copy of personal data for a given retention period[73]. A 2023 overview over the diffusion of such right around the world has counted 57 jurisdictions (in addition to six US States and one Canadian province) that have introduced a statutory right to data portability in some form, even though 5 of them (and 5 US States) only recognize an indirect or intermediated portability[74]. The United Kingdom went further than personal data in 2025 with the adoption of the Data Use and Access Act, which enables the Secretary of State to make regulations to require the suppliers of goods or services to provide customer data and business data to a

70 European Union, 'Charter of Fundamental Rights of the European Union', 2012/C 326/02, 26 October 2012. Available at http://data.europa.eu/eli/treaty/char_2012/oj. Accessed 4 dec. 2025.

71 Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms' Council of Europe Treaty Series 005, Council of Europe, 1950.

72 Section 26 h (5) (a) of the Personal Data Protection Amendment Act of 2020.

73 Yeong, Zee Kin, and David Roi Hardoon, 'Taking Your Data with You: Singapore's Approach to Data Portability', in Linda Jeng (ed.), *Open Banking* (New York, 2022; online edn, Oxford Academic, 24 Mar. 2022), https://doi.org/10.1093/oso/9780197582879.003.0007, Accessed 26 Feb. 2026

74 Lienemann, Gregor, Global Perspectives on the Right to Personal Data Portability: Surveying Legislative Progress and Propositions for User-Led Data Transfers (April 21, 2023). Available at SSRN: <https://ssrn.com/abstract=4427736> or <http://dx.doi.org/10.2139/ssrn.4427736>. Accessed

customer or an authorized third party in "real time"[75].

There is also more legislation in the European Union, other than data protection law, that creates, complements or enhances the right to data portability. For instance, the revised Payment Services Directive[76] provides for the right of bank account holders to transfer data from their payment account to third-party providers. As a complement, Art. 14 of the Digital Content Directive[77] gives consumers who terminate a contract for digital content or service the right to retrieve, free of charge, in a reasonable time and in a machine-readable format, without hindrance from the trader, any content other than personal data which was provided or created by them when using the digital content or service supplied by the trader. And the Regulation on the Free Flow of Personal Data[78] encourages the development of self-regulatory codes of conduct to make it easier for professional users to switch providers of data processing services and to port data.

Most recently, EU legislation introduced two different types of data portability, in the Digital Markets[79] Act and the Data Act[80]. The former establishes it as an obligation for gatekeepers[81] under art. 6(9)[82], upon

75 See Part 1, art. 1-26.

76 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), *OJ L 337, 23.12.2015, p. 35-127.*

77 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. PE/26/2019/REV/1, OJ L 136, 22.5.2019, p. 1–27.

78 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59.

79 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**.** Official Journal on October 12, 2022 (OJ L 265, 12.10.2022, p. 1–66). Available at: http://data.europa.eu/eli/reg/2022/1925/2022-10-12. Accessed 4 dec. 2025.

80 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 and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). OJ L, 2023/2854, 22.12.2023, Available at: http://data.europa.eu/eli/reg/2023/2854/oj. Accessed 4 dec. 2025.

81 According to Article 2(1) DMA, "'gatekeeper' means an undertaking providing core platform services, designated pursuant to Article 3". The undertaking will be designated as gatekeeper if it attends to the Article 3 DMA criteria.

82 "The gatekeeper shall provide end users and third parties authorized by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise

request of end users or authorized third parties, for all user-generated data (personal and non-personal, including inferred data, and including by the provision of continuous and real-time access to such data). Similarly, art. 6 (10) provides business users with continuous access, free of charge, to all data generated by the gatekeeper on interactions between end users and the platform of that specific business user, including personal data of those end users, provided that they give explicit consent. However, like the GDPR, the DMA does not define standards for ensuring an effective exercise of data portability, though it includes in its recital (97) a reference to the possibility to use of technical standards to facilitate data portability and interoperability, and for the Commission to request their development to European standardization bodies where appropriate and necessary. The latter, in its Chapter II (Articles 4 and 5) introduces a horizontal data access right, encompassing personal and non-personal data generated by connected products, and a right to transfer the data to third parties "without undue delay, free of charge to the user, of the same quality as is available to the data holder". It also clarifies that any user that requests data access shall not use it to develop a product that competes with the product from which the data originate, and contains restrictions (under art 5) for the recipients of portability requests (including the ability of "gatekeepers" to request such data). It also forbids third parties from requesting certain conditions or providing the data in particular manners (under art. 6)[83].

Similar obligations may be imposed pursuant to the updates to competition law that have been introduced in other jurisdictions to deal with the challenges of digital platforms. For example, article 19a of the

of such data portability, and including by the provision of continuous and real-time access to such data".

83 Specifically: (a) coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user; (b) use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of the GDPR, unless it is necessary to provide the service requested by the user; (c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user; (d) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper pursuant to Article [...] of [Regulation on contestable and fair markets in the digital sector (Digital Markets Act)]; (e) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose; (f) prevent the user, including through contractual commitments, from making the data it receives available to other parties.

German Act against Competition Restraints (GWB) includes amongst the prohibited conduct by companies with paramount importance across markets the refusing the interoperability of products or services or data portability, or making it more difficult, and in this way impeding competition; and section 20 (3) of the Digital Markets, Competition and Consumers Act 2024 in the United Kingdom includes conduct requirements that prevent an undertaking with strategic market status from using its position in relation to the relevant digital activity, including its access to data relating to that activity, to treat its own products more favorably than those of other undertakings; and restricting interoperability between the relevant service or digital content and products offered by other undertakings. Indeed, the Competition and Markets Authority recently opened a consultation on the proposed conduct requirements on data portability applicable to Google's general search[84]. The Japanese Mobile Software Competition Act also contains in its Art. 11 a provision requiring data portability, covering basic operating software data on the user's contact information, App Store information on the individual software, and browser information[85].

As discussed above, there are several limitations in the scope and application of data portability, which may hinder its effectiveness. Even under in its most wide-ranging form, data portability may be considered a relatively "lightweight" remedy because its effects depend on active behavior by consumers (which may be insufficient to overcome the networks effects[86] enjoyed by the incumbent) and the ultimate goal may be frustrated by the lack of legal standards over how data may be transferred from one provider to another in order to lose its value. Not surprisingly, it is often combined with mandated interoperability, which is addressed in the following section. Indeed, while the right to

84 See <https://assets.publishing.service.gov.uk/media/6979ce981c24881f40a4d6dd/_Data_portability_conduct_requirement_v2.pdf>. Accessed 30 March 2026.

85 See <https://laws.e-gov.go.jp/law/506AC0000000058/20251218_000000000000000>. Accessed 30 March 2026

86 Network effects may be either direct or indirect. According to *Cadernos do Cade sobre Mercados de Plataformas Digitais* (2021), positive direct effects are those in which "the utility for users derives from the number of users on the same side, which constitutes the direct network effect"; however, negative effects may also arise in certain platform contexts. Indirect and positive effects, in turn, occur when "one group of users benefits more as the number of members in another group increases and, possibly, vice versa. Thus, if the platform provides a better service on one side of the market, demand for that service increases on the other side".

data portability is typically provided under data protection legislation, its effectiveness may remain limited in the absence of agreed upon standards: this is the case, for instance in the EU[87], concerning what constitutes a "structured, commonly used and machine-readable format" or, in Brazil, where legislation attributes to the data authority the competence to establish interoperability standards[88]. If this is achieved through standardization, as suggested by EU legislation, it is also important to craft the rules in a way that prevent incumbents from using this procedure as a way to raise rivals' costs[89].

Application

In addition to the proliferation of the right to data portability in legislation, on can see an increasing adoption of data portability as a remedy in competition cases.

One notable example involves a **decision by CADE in a proceeding against Bradesco**, a bank that was investigated for allegedly raising obstacles to portability of customers' account data to fintech provider Guiabolso[90]. CADE investigated the conduct in particular insofar as it required fintechs an additional token to access certain areas of the customers' Internet banking.

The case was settled in October 2020 with the adoption of a term of conduct cessation ("TCC")[91], broadly equivalent to a commitment decision, where Bradesco committed to:

> (i) develop connection interfaces that enable Guiabolso to request and obtain consent from its users that are Bradesco's customers, and to access via previously established encrypted communication to Bradesco's

87 WONG, J., HENDERSON, T., ´The right to data portability in practice: exploring the implications of the technologically neutral GDPR´, International Data Privacy Law, Volume 9, Issue 3, August 2019, Pages 173–191, <https://doi.org/10.1093/idpl/ipz008>. Accessed 30 March 2026

88 Art. 40 of the Brazilian data protection law (LGPD).

89 Gal, M. S., & Rubinfeld, D. L. (2019). Data standardization. New York University Law Review, 94(4), 737-770

90 Administrative Procedure No. 08700.004201/2018-38.

91 Cease and Desist Agreement No. 08700.003425/2020-47.

system in a way that allows collection of all data from users that have provided consent;

(ii) submit a report within 30 days containing the technical documentation made available for interconnection, the interactions occurred with Bradesco for testing purposes, and the documentation that demonstrates the effectiveness of the consent interface;

(iii) the deposit of $ 23.878.716,72 into the collective defense fund; and

(iv) the withdrawal of the legal action initiated by Bradesco for violation of bank secrecy and unfair competition.

It is important to highlight that this case occurred prior to the adoption of sector-specific legislation as part of the so-called Open Finance, which was introduced in Brazil in 2020. It could be said that the Guiabolso case paved the way for open banking in Brazil, drawing attention to the mechanisms that incumbent banks were expected to develop in order to facilitate the porting of customer data.

A second interesting case involves the Japanese competition authority, the **Japanese Fair Trade Commission** (JFTC), issuing a cease-and-desist order against **MC Data Plus**[92]. Since 2015, MC Data Plus has offered cloud-based services for the construction industry (the "*kensetsu-site series*"). Among its principal services, it provides a labor-safety service known as "GREEN-site," which requires users to register their employee information and other data to access the platform. When users wish to migrate to another labor-safety service, however, they must re-enter and re-register the same employee data on the new platform. Because the information required for each employee may exceed 100 individual data fields, this process imposes a substantial burden on firms with large workforces.

92 Japan Fair Trade Commission (JFTC), Cease and Desist Order against MC Data Plus Co., Ltd. (24 December 2024) at <https://www.jftc.go.jp/houdou/pressrelease/2024/dec/241224nijo.html>. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

According to the JFTC, MC Data Plus considered the protection of the employee information and other data stored in GREEN-site against access by new entrants in the labor-safety service market to be essential for maintaining the competitive advantage of its services and, to that end, the company adopted measures that discouraged users from switching to competing services. One such measure consisted of refusing requests from GREEN-site users to obtain their employee information in a format compatible with other labor-safety platforms they wished to use – even though the data had been originally provided by the users themselves. MC Data Plus denied these requests without reasonable justification, invoking grounds such as personal-information protection. Therefore, the JFTC issued a cease-and-desist order pursuant to the Japanese Antimonopoly Act. The order required the company to refrain from refusing, without legitimate grounds, to provide users with the information they had themselves provided to the services offered by MC Data Plus[93]. It is worth mentioning that, prior to issuing the order, the JFTC consulted the data protection authority, Personal Information Protection Commission, which confirmed that the designed remedy did not conflict with the Act on the Protection of Personal Information[94]. Litigation challenging the cease-and-desist order is currently pending.

A third interesting case is the 2021 decision by Italian competition authority – **Autorità Garante della Concorrenza e del Mercato (AGCM)[95]**–making binding the commitments offered by **Google**[96] to solve competition concerns on data portability. Triggered by a complaint filed by Hoda, the AGCM initiated an investigation against Google to ascertain potential violations of Article 102 TFEU, consisting of obstacles created by Google to the identification of appropriate interoperability mechanisms capable of making the data held on its platform available to alternative platforms. Hoda stated that it had initiated contacts with

93 Japan Fair Trade Commission (JFTC), Press Release. 'The JFTC Issued a Cease and Desist Order to MC Data Plus, Inc.' (24 December 2024) at https://www.jftc.go.jp/en/pressreleases/yearly-2024/December/241224.html. Accessed 30 March 2026

94 Act on the Protection of Personal Information Act No. 57 of May 30, 2003. Available at https://www.japaneselawtranslation.go.jp/ja/laws/view/4241. Accessed 30 March 2026

95 The relevance of this case was suggested by the Italian competition authoirity in response to the questionnaire.

96 Case no. A552 – Google-Obstacles To Data Portability, 2023 commitment decision.

Google to identify interoperability mechanisms that would allow users of its "Weople" platform to transfer there (pursuant to Article 20(2) of the GDPR) the data held within Google's ecosystem. However, Google indicated that the only way it makes available to users to request and obtain a copy of their data is its "Takeout" service.

According to AGCM, the alleged abusive conduct involved, in particular, the creation of interoperability barriers in data sharing with other platforms, limiting users' ability to use and benefit from their data through alternative services[97]. From the three commitments offered by Google, two involved solutions related to Takeout to facilitate data export to third-party operators, namely by providing an URL that could be embedded in third-party sites bringing to Takeout, and expanding the categories of data subject to portability (including browsing history and Youtube). The third allowed early testing of a new direct data portability solution (via Application Program Interface, or API[98]) between services, for third-party operators, upon request and authorization by end users, concerning data provided by the users themselves or generated through their activities on Google's search engine and YouTube. Remedies were meant to (i) facilitate the portability of users' data, (ii) improve the usefulness of data exported and shared by users with third-party operators, and (iii) accelerate the effective adoption of a new solution for direct data portability from service to service, which Google will make available to third-party operators authorized by an end user whose data is the subject of the portability request relating to certain Google products. In other words, the commitments encompassed the adoption of mechanisms designed to facilitate the export of data to third-party operators and to ensure easier access to the personal data generated

97 See Case no. A552 – Google-Obstacles To Data Portability, 2023 commitment decision, para 7-9 at: https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/42A8996C723B26AAC12589FD003925C3/$File/p30736.pdf.

98 "APIs are tools and protocols that allow computers to easily communicate with each other (Jacobson et al., 2011). Web accessibility allows public APIs to serve as conduits to business processes that the firm itself controls. APIs offer the dual virtues of practical modular design and precise metering of access, foundations of a digital ecosystem". Cf. Benzell, Seth and Hersh, Jonathan Samuel and Van Alstyne, Marshall W. and Lagarda, Guillermo, 'How APIs Create Growth by Inverting the Firm' (August 5, 2019). Available at: <https://ssrn.com/abstract=3432591>, p. 2. Accessed 30 March 2026

by users through their interactions with Google's services[99]. However, at the time this Report was written, the public record does not reveal any formal coordination between AGCM and the Italian data protection authority for purposes of this particular case.

In the United Kingdom, data portability measures have been proposed not as a competition remedy but as a conduct requirement (CRs) under the Digital Markets, Competition and Consumers Act 2024 (DMCCA). Following the designation of **Google** in October 2025 as having "strategic market status" (SMS) in the provision of general search and search advertising (general search services), the **Competition and Markets Authority (CMA)** launched, in January 2026, a consultation on **proposed CRs** applicable to these services[100].

One of these requirements concerns data portability, aiming to "ensure that UK consumers who use Google's general search services can effectively port their data to other businesses to develop new services or otherwise share the value of that data." The main concerns raised by stakeholders are related to the voluntary nature of the implementation of the API in the UK, focusing on operational uncertainty and several aspects of the technical implementation and service levels provided by Google. With respect to operational uncertainty, as the API is not mandatory under UK law, some worried that it could be withdrawn at any time. Providing legal certainty would presumably reduce barriers to investment in applications that rely on data made available through the API. Regarding technical aspects, the issues raised included security verification, operational predictability, reliability and scalability, and consent flows (including the presence of several consent screens), among others.

To address those concerns related to data portability, the CMA proposes, as conduct requirements, that Google "provide third parties authorized by a UK End User, at their request and free of charge, with tools to facilitate the effective portability of Specified Data" and "comply

99 See AGCM, 'A552 - Italian Competition Authority: Following the Authority's intervention, Google's data portability becomes easier', Press Release (31 July 2023), at <https://en.agcm.it/en/media/press-releases/2023/7/A552>. Accessed 30 March 2026

100 https://www.gov.uk/government/consultations/googles-general-search-services-proposed-conduct-requirements.

with its obligations under this conduct requirement by making its DMA Data Portability API available in relation to UK End Users on the same terms and to the same standard as within the European Economic Area." To support this objective, the CMA will publish Interpretative Notes, which propose that Google, in order to ensure the effectiveness of its data portability tools, must:

> (a) maximize any data portability tool's uptime, ensure that data transfers under any data portability tools are successful and ensure that data ported under any data portability tool is complete, accurate, and sufficient to enable any authorized third party to match it with the UK End User;
>
> (b) provide sufficient capacity to allow authorized third parties to access data at a frequency that meets their reasonable business needs;
>
> (c) provide appropriate and understandable error messages to authorized third parties if they are denied access to the underlying data;
>
> (d) maintain its existing issues tracker or provide an alternative, sufficiently resourced channel that enables authorized third parties to report issues;
>
> (e) address issues identified through the issues tracker or alternative channel as quickly as practicable;
>
> (f) give sufficient notice to authorized third parties and UK End Users of any material changes to the data portability tools;
>
> (g) ensure that UK End Users are presented with balanced, understandable, and appropriately targeted choices across all data portability tools and, while recognizing that data portability is itself an important data protection right, ensure that consent flows appropriately balance ease of data portability with privacy and security considerations; and

(h) ensure that, if third-party applicants are required to undergo an approval and verification process to demonstrate that they have adequate security arrangements in place to protect user data before accessing data portability tools, (i) any verification process can be undertaken in a timely and effective manner and does not impose unreasonable requirements or administrative or other costs on third-party applicants and (ii) approval to use the data portability tools provided by Google, such as the DMA Data Portability API, is not conditional upon restrictions on the use of the data by the third-party applicant, and this is clearly communicated.

Following the CMA's proposal, data portability requirements will be monitored through three mechanisms: (i) ongoing stakeholder engagement and feedback; (ii) reporting of key metrics by Google; and (iii) an annual compliance report submitted by Google. The CMA proposed requiring Google to provide the following metrics in each compliance report, each relating to UK-based usage of the data portability solution during the reporting period and disaggregated by month: "(a) the percentage of requests successfully served via the API; (b) the percentage of data exports completed via the API within 24 hours; (c) the percentage of files successfully exported in completed requests via the data portability API; (d) the percentage of API uptime in each 24-hour period; and (e) the number of users who initiated a data export via the API. These monitoring tools would ensure effective implementation of Google's solutions."

(ii) Mandated interoperability

Definition

One frequent remedy in digital markets, said to be suitable to address concerns related to leveraging and to undo the competitive impact of network effects, is interoperability, which refers to the imposition of obligations to ensure that the information technology (including the

relevant data) of the concerned undertaking(s) remains interoperable with the products of competitors[101]. Some scholars and competition authorities suggest that not only can this obligation facilitate the attainment of minimum scale for competitors in downstream markets (vertical interoperability), but it may also enable multi-homing in the same relevant market (horizontal interoperability)[102].

In this sense, interoperability can be defined as the ability to transfer and render useful data and other information across systems, applications, or components[103]. The combination of transmission and analysis involves several layers of the so-called Open Systems Interconnection model (OSI model)[104], requiring the achievement of various levels of interoperability[105]. At a minimum, one should distinguish the lower and the upper layer, pointing to a division between infrastructural interoperability and data interoperability. While infrastructural interoperability enables IoT devices to exchange data under common network protocols, data interoperability concerns more directly users and developers of IoT applications, allowing them to meaningfully connect the interfaces of those applications.

101 See EU Remedy Notice, para. 65.

102 Wolfgang Kerber and Heike Schweitzer, Interoperability in the Digital Economy, 8 (2017) JIPITEC 39 para 1.

103 GASSER, U. ´Interoperability in the Digital Ecosystem´, Berkman Center Research Publication No. 2015-13 July 6, 2015. Available at SSRN: http://ssrn.com/abstract=2639210

104 Open Systems Interconnection model (OSI Model) is a conceptual model that defines a unifying standard for the architecture of networking systems. For more information, see http://www.tcpipguide.com/free/t_TheOpenSystemInterconnectionOSIReferenceModel.htm

105 More specifically, the interoperability required at the different layers concerns the following:
-At the physical layer (#1), the definition of hardware specifications; the transformation of local data into bits that can be sent over the network; and the actual transmission of those data over the network.
- At the data link layer (#2), the establishment of the functions required for the establishment and control of logical links between local devices on a network; and the procedures used by devices to control access to the network medium.
- At the network layer (#3), the logical addressing and the routing of data across a series of interconnected networks.
- At the transport layer (#4), ensuring that various software applications can all send and receive data using the same lower-layer protocol implementation.
- At the session layer (#5), ensuring the persistent logical linking of two software application processes, to allow them to exchange data over a prolonged period of time.
- At the presentation layer (#6), compressing, encrypting and translating different formats of representing data.
- At the application layer (#7), implementing the functions that are needed by users of the network and issuing the appropriate commands to make use of the services provided by the lower layers.

At the infrastructure (lower) layer, interoperability is achieved through the use of common protocols for the conversion, identification and logical addressing of data to be transmitted over a network. The most common standards in this layer are Ethernet and TCP/IP. Protocols are also used for communication between computer programs over telecommunications equipment, through common languages such as HTTP for web content, and STMP, IMAP and POP3 for emails[106]. At the application (upper) layer, interoperability is attained by reading and reproducing specific parts of computer programs, called interfaces, which contain the information necessary to "run" programs in a compatible format. However, different interfaces are needed depending on who actually "runs" the program[107]: if it is from the perspective of the user/consumer of the computer program, user interfaces are relevant to the extent that they enable them to visualize and deploy a specific set of commands or modes of interaction with the program that can potentially be replicated into another (different) application. Importantly, although this kind of interoperability can increase a program's utility to the user, it is not *required* for the purpose of its technical functioning.

Most choices for user interfaces seem to be dictated not so much by functional elements of the program, as by the pursuit of the goals of user friendliness, aesthetical appeal and promotion of brand-specific features[108]. It is said that[109], from the perspective of the developer of a computer program, the relevant interfaces for interoperability are the APIs, i.e. any well-defined interfaces which define the service that one component, module or application provides to other software elements. At the same time, interoperable APIs do not necessarily imply the ability of either users or developers to meaningfully relate the outputs of

106 VAN ROOIJEN, A., *The Software Interface between Copyright and Competition Law: A Legal Analysis of Interoperability in Computer Programs* (Kluwer Law, Alphen aan den Rijn 2010).

107 According to the Posix Open Systems Reference Model, these interfaces can be of four types: (a) Human/computer interface services; (b) Information interchange services; (c) Communication services; and (d) Internal system services.

108 VAN ROOIJEN, A., *The Software Interface between Copyright and Competition Law: A Legal Analysis of Interoperability in Computer Programs* (Kluwer Law, Alphen aan den Rijn 2010).

109 DE SOUZA, C. et al., ´Sometimes You Need to See Through Walls- A Field Study of Application Programming Interfaces´, in Computer supported cooperative work, ACM Press 2004, p. 63-71.

interoperable computer programs, unless they are expressed in the same language (most commonly, JPEG for images, HTML for webpages, PDF for documents and MP3 for music). Scholars suggest that this can be achieved through the so-called "data interfaces", which are responsible for restoring and retrieving data in a specific format[110].

Both legal and technical constraints must be taken into account for the attainment of the more comprehensive notion of "effective" interoperability. In particular, interoperability information can be protected through a patent, copyright, or a trade secret. Furthermore, copyright and database protection can be used to control the use of data or data structures taken from another provider. Finally, data protection law may determine the extent to which information can be extracted and re-utilized without the consent of the data subject, and therefore potentially constitutes a further obstacle to lawful interoperability. Interoperability might be implemented, for instance, in a way that lets third parties immediately see and interact with the users of a company without their prior knowledge or consent, which is likely to generate data privacy issues. Accordingly, the design of the remedy will need to consider how to ensure that the assertion of rights over information does not unduly hamper its effectiveness.

There are other equally important issues to be considered relating to the implementation of interoperability as an antitrust remedy. First and foremost, its scope, particularly concerning involved stakeholders (both on the providing and on the receiving end) and of the resources that are made to be interoperable. This is an important question, as casting too wide a net may create a disincentive away from the development of differentiating services due to the availability of an equivalent input from an incumbent. Secondly, the timing and frequency under which interoperability can be requested, as this can influence both the costs of this intervention for an incumbent and the extent to which it is apt to serve the needs of competitors in a dynamic market setting. Third, the effectiveness of interoperability remedies may also depend on the

110 VAN ROOIJEN, A., *The Software Interface between Copyright and Competition Law: A Legal Analysis of Interoperability in Computer Programs* (Kluwer Law, Alphen aan den Rijn 2010).

existence of a dispute resolution mechanism and the availability of information to third parties regarding prior requests for interoperability, as well as the Key Performance Indicators for existing requests and any dispute resolution. Fourth, a key question regards the possibility to request a fair and proportionate remuneration, something that was recently recognized by the EU case-law (with a view to allowing the undertaking to derive an appropriate benefit, considering the actual costs to be incurred),[111] but explicitly discarded by article 6 (7) and 7 (1) of the DMA. By contrast, the DMA in articles 6 (11) and 6 (12) establishes the application of FRAND conditions for access to ranking, query, click and view data for competing search engines, and for access to software application stores, online search engines and online social networking services.

Padilla and Prasad have examined FRAND in article 6 (12), suggesting that the calculation of rates in the latter scenario ought to cover the long run average incremental costs of the gatekeeper's business, without considering the network effects, and reduced by the value perceived by each specific gatekeeper through the operation of the service (for instance, through data accumulation)[112]. In turn, regarding article 6 (11), both Krämer[113] and Van den Boom[114] affirm that FRAND may imply zero costs, as there may be no LRAIC-equivalent for a business that is monetized through advertising. Krämer considers that this may be fair for competitors of a certain size[115], while Van den Boom goes as far as saying that the starting point should be that access to click & query data is free, unless the gatekeeper justifies otherwise, on the basis of the situation of the prospective recipient[116]. These discussions may be useful to inspire similar parameters when it comes to interoperability and data sharing obligations more broadly.

111 C-233/23, *Android Auto (Enel X)*. ECLI:EU:C:2025:110.

112 Jorge Padilla and Kadambari Prasad, Taking Article 6 (12) DMA Seriously: FRAND Access Prices for App Stores., SSRN Electronic Journal (2025), 5-8. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5261312. Accessed 30 March 2026.

113 Krämer J., Data Access Provisions in the DMA, CERRE Report (2022), 15-16.

114 Van den Boom, J.. The Search for Meaningful Results: FRAND Access Conditions under Article 6(11) DMA. European Competition Regulatory Review4|2025, 302-319.

115 Id., at 26.

116 Id., at 315.

Application

Interoperability obligations have been imposed long before the advent of the digital age: for instance, the US Supreme Court in 1912 required a group of railroad companies that jointly owned a bridge across the Mississippi River to give competing railroad companies fair access to the bridge and the ability to interconnect on both sides of it[117]. In 1982, as a remedy to repeated attempts by American Telephone & Telegraph to frustrate the interconnection of MCI Communications (a long-distance company who needed access to the local loop to provide added value services), the US government imposed a breakup AT&T into the seven regional Bell operating companies (RBOC)s and a smaller new central division. RBOCs were requested to allow independent long-distance firms equal access to the local exchange and to abstain from engaging in any business other than common carriage as defined in the telecommunication legislation, including to expand beyond the regional level, which favored the rise of a national network based on interoperability standards[118].

However, these early cases concerned purely physical interconnection, whereas many of the modern cases have to do with information technology- and thus, the compatibility between data processing systems.

United States of America

A famous remedy opening the discussion on interoperability in this context in the **United States** was the one adopted in the *Microsoft* case[119], where Microsoft had been found guilty for tying its browser to its operating system Windows. Microsoft was required to grant access on FRAND terms to its APIs,

117 *United States v. Terminal R.R. Ass'n,* 224 U.S. 383 (1912).

118 SCOTT MORTON, F. KADES, M. , ´Interoperability as a Competition Remedy in Digital Networks´ (March 19, 2021). Available at SSRN: <https://ssrn.com/abstract=3808372> or <http://dx.doi.org/10.2139/ssrn.3808372>. Accessed 30 March 2026.

119 *United States v Microsoft* No 98-1232, 2009 WL 1348218 *6 (DDC 22 Apr 2009). See <https://www.justice.gov/atr/case/us-v-microsoft-corporation-browser-and-middleware>. Accessed 30 March 2026.

related technical information and communication protocols, which its Middleware (a software that enables communication and data management between an operating system and the applications running on it) utilizes to interoperate with Windows. In conjunction with that, the remedy enjoined from restricting by agreement any OEM licensee from installing an icon, menu entry, shortcut, product, or service related to "Non- Microsoft Middleware" and to allow both Original Equipment Manufacturers (OEMs) and end users to disable end-user access to various types of Windows functionality. Furthermore, it prohibited Microsoft from designing its operating system product so as to induce reconfiguration of an OEM's or consumer's formatting of icons, shortcuts, and menu entries in an attempt to favor Microsoft's own software.

What is not often discussed about the implementation of this remedy is the technical complexity of this task, especially in regard of the requirement to prepare and provide the necessary communications protocols ("CPs") to would allow non-Microsoft servers to communicate with Windows clients, ordered to be provided within the first 3 years of the 5-year term of the consent order. Due to issues of technical feasibility, Microsoft obtained two 2-year extensions, after which "the Justice Department and the outside parties effectively gave up, agreeing to declare Microsoft's work "substantially complete" although there remained hundreds of unresolved technical issues"[120]. Data privacy considerations may have played a role in this regard, as the consent decree carved out a specific exception for disclosures that would compromise data security, the security of its anti-virus or other security systems[121]. Therefore, the absence of a robust framework to assess these justifications may have contributed to the limited

120 J. Kwoka, T. Valletti Unscrambling the eggs: breaking up consummated mergers and dominant firms; Vol. 30 (5) Industrial and Corporate Change, 2021.

121 Douglas, Erika, U.S. Antitrust Remedies and Data Privacy (May 01, 2025). Temple University Legal Studies Research Paper Forthcoming, Available at SSRN: <https://ssrn.com/abstract=5400893> or <http://dx.doi.org/10.2139/ssrn.5400893>. Accessed 30 March 2026.

progress Microsoft made in the implementation of the remedy.

A second notable decision in the United States, which illustrates the difficulties of access remedies involving interoperability and data portability is *United States v Bazaarvoice*,[122] where the **US Department of Justice (DOJ)** challenged the **acquisition of PowerReviews**, the second biggest provider in online product ratings and review services, **by market leader Bazaarvoice**. The remedy adopted included not only the divestiture of PowerReviews, but also the granting of non-discriminatory access for four years to Barzaarvoice's syndication network. In other words, the interoperability of PowerReviews´ ratings and reviews with Bazaarvoice´s add-on feature allowed manufacturers and retailers to incorporate such information into their product offerings.

At the end of a four-year period, the district court issued an order bringing the remedy to an end, observing the existence of "innumerable complex issues to resolve"[123]. Amongst those, one of the monitoring trustees cited the need for both the sender and the receiver of data transfers to create a system to address data conversion issues and to track their resolution, for adequate measures to protect against possible hacking of the data flows, and for "moderation" of some of the data received before displaying it on a public-facing website (for instance, to prevent it from revealing sensitive competitive information or upsetting privacy expectations)[124].

A third and more recent US decision involving interoperability is the **US District Court for the District Columbia (judge Mehta)'s decision** on remedies relating to the **Google** distribution practices with OEMs[125]. Here, the idea of

122 *United States v. Bazaarvoice, Inc.,* No. 13-cv-00133-WHO, 2014 WL 203966 (N.D. Cal. Jan. 8, 2014)

123 Order Administratively Closing the Case, *United States v. Bazaarvoice, Inc.*, No. 13-cv-00133-WHO (N.D. Cal. Aug. 28, 2018), ECF No. 394.

124 HIMES, J., NIEH, J., SCHNELL, R., ´Antitrust Enforcement and Big Tech: After the Remedy Is Ordered´. Stanford Computational Antitrust 1 (5), 20, 2021. 2021

125 See <https://storage.courtlistener.com/recap/gov.uscourts.dcd.223205/gov.uscourts.

"syndication" was used to oblige Google to offer third-parties a licensed use of its own services to boost their own search solutions, by giving them "latency, reliability, and performance functionally equivalent to what Google provides for Search Text Ads on its own SERP" (Search Engine Results Page). In particular, for purposes of granting effective interoperability, Plaintiffs demanded Google to provide the following data:

> (i) Data sufficient to understand the layout, display, slotting, and ranking of all items or modules on the SERP, including but not limited to the mainline content and sidebar content and sitelinks and snippets;
>
> (ii)Ranked organic search results obtained from Google database or index, regardless of whether such web content was obtained by crawling the Internet or by other means;
>
> (iii)Search features that enable query corrections, modification, or expansion like spelling, synonyms, autocomplete, autosuggest, related search, "did you mean," "people also ask," and any other important query rewriting features identified by the Technical Committee;
>
> (iv)Local, Maps, Video, Images, and Knowledge Panel[126] search feature content; and
>
> (v) FastSearch results (fast top organic results).

The proposed remedy also required that Google imposes no restrictions on use, display, or interoperability with Search Access Points, including of GenAI Products, provided, except for reasonable steps to protect its brand, its reputation, and security. While the Court accepted the gist of this remedy, it

dcd.223205.1436.0_1.pdf>. Accessed 30 March 2026.

126 According to Google, "Knowledge panels" are information boxes that appear on Google when you search for entities (people, places, organizations, things) that are in the Knowledge Graph. In turn, is a tool offered by Google enables you [users] to search for things, people or places that Google knows about—landmarks, celebrities, cities, sports teams, buildings, geographical features, movies, celestial objects, works of art and more—and instantly get information that's relevant to your query. See <https://support.google.com/knowledgepanel/answer/9163198?hl=en> and <https://blog.google/products-and-platforms/products/search/introducing-knowledge-graph-things-not/>. Accessed 30 March 2026.

narrowed it in important ways. Perhaps most importantly, it restricted the scope of syndication to data that is obtained by crawling the Internet (not derived from third parties or from other Google products or services). It did so noting that (i) not only is the proposed scope beyond what is appropriate to close the scale gap, but (ii) there is no evidence of search syndicator offers that go so far; and (iii) in cases where there is an established market concerning the action that is required by the remedy, it is best to hew closely to ordinary commercial terms. The same applies to the requirement to share at "marginal costs" or the prohibition to place any conditions on how any licensee may use syndicated content: ordinary commercial restrictions on use (including those to protect its IP and against spam and malware) are permitted. The Court also reduced the duration to 5, instead of 10 years, consistent with the objective of the remedy to serve as a near-term solution and capped to 40% of annual queries the requests that can be done by Qualified Competitors, leaving it to the Technical Committee to establish the percentage cap in the following years.

Italy

Another landmark case is **Android Auto**[127], which gave rise to a decision **by the Italian competition authority (AGCM),** an appeal decision and ultimately a decision by the European Court of Justice. By way of background, Enel X Italia filed a complaint against Google for refusing to allow its electric vehicle charging point location application to operate on Android Auto, Google's own operating system for cars that integrates applications into a vehicle's dashboard interface. According to the complaint, this refusal unjustifiably limited users' options and favored Google's own ecosystem, particularly its navigation

127 See Decision A529, Alphabet Inc, Google LLC and Google Italy Srl, Decision of 27 April 2021, available at <https://www.agcm.it/dotcmsdoc/allegati-news/A529_chiusura.pdf>, para 444 and p. 154. Accessed 30 March 2026.

services, which already offered functionalities related to electric vehicle charging. Google justified the restriction on grounds of safety concerns and argued that, at that time, only media and messaging applications were compatible with the platform. Subsequently, following the initiation of proceedings, Google began providing experimental (beta) tools to enable the development of electric vehicle charging applications compatible with Android Auto, but uncertainty remained over the eventual release of the final version of this template and the effective ability to allow the development of full functionalities, including the booking and the starting of the recharge session.

The AGCM found that Google's conduct constituted an abuse of dominant position, as it hindered the entry of competing applications into the market. The authority considered Android Auto to be an essential infrastructure, indispensable for effective competition in the relevant market, and concluded that the refusal to ensure interoperability had anticompetitive effects. As a result, a fine exceeding €100 million was imposed on Google. In addition to the financial penalty, the Authority ordered Google to implement corrective measures to ensure interoperability and restore competitive conditions. In particular, Google was required to:

> (i) release the final version of the template for the development of electric vehicle charging applications;
>
> (ii) where the template did not enable the development of the Enel X Italia application with all functionalities deemed essential, develop the missing functionalities by integrating the existing template or creating a new one; and
>
> (iii) within thirty days of notification of the decision, submit to the Authority a proposal for the appointment of a trustee responsible for overseeing the implementation and monitoring of the obligations, and grant that trustee

access to all information and resources necessary for the proper execution of its duties.

The case made its way to the European Court of Justice through a preliminary reference raised by Italy's highest administrative law tribunal (*Consiglio di Stato*), resulting in an important ruling on the scope of the essential facility doctrine under EU competition law[128]. Most relevant for our purposes is the part in which the Court deals with the concern of insufficiency of the template that existed to obtain effective interoperability. The decision affirms that Article 102 TFEU must be interpreted as meaning that the undertaking in a dominant position is required, first, to take into consideration the general needs of the market or the needs of the undertaking requesting that access and, second, to inform that undertaking of the time necessary to develop that model or whether the competition authority is required to verify, on the basis of objective evidence, the time necessary for the undertaking in a dominant position to develop such a template[129].

In this context, the Court is clear that a refusal may be objectively justified where to grant such interoperability by means of such a template would, in itself and in the light of the properties of the app for which interoperability is sought, compromise the integrity or security of the platform concerned, or where it would be impossible for other technical reasons to ensure that interoperability by developing such a template. However, the fact that there is no template for the category of apps concerned or the difficulties involved in its development which the undertaking in a dominant position may face cannot in themselves constitute an objective justification for that undertaking's refusal to grant access. It then indicates what it considers the elements of particular relevance in making determination over the development of a

128 Judgment of 25 February 2025, *Alphabet and Others (Android Auto),* C-233/23, EU:C:2025:110.

129 Para. 69.

template, in particular (i) the degree of technical difficulty in developing the template for the category of apps concerned, which permits the access requested, (ii) constraints related to the fact that it is impossible for it to equip itself, within a short time, with some of the resources, in particular human resources, necessary to develop that template in the light of the needs of the undertaking requesting that access, or even (iii) constraints external to the undertaking in a dominant position which have an impact on its ability to develop that template, such as, for example, constraints relating to the applicable regulatory framework.[130]

It is worth noting that the obligation to provide a development template primarily promotes syntactic and semantic interoperability, as it establishes the technical specifications and interface protocols necessary for third-party applications to communicate with the Android Auto platform. Furthermore, it is interesting to highlight that no discussion can be found in the public version of the decision regarding the possible responsibilities of the two parties in relation to data processing. In this sense, one could argue that the remedy might raise concerns from a data protection perspective, particularly insofar as the remedy grants access to user data for third parties who are not trustworthy that should have been addressed. Nonetheless, one can also argue that, in principle, these concerns should be addressed through the fulfillment of regulatory requirements that fall outside of the competition authority jurisdiction. Hence, the fact that a remedy may contribute to raising a risk under data protection and cybersecurity can be understood as a relevant factor that might warrant more dialogue between competition and data protection authorities.

130 Para. 72-75.

European Union

Moving to the European Union, a decision for interoperability purposes is the one taken by the **European Commission against Microsoft** in 2004[131]. After a five-year investigation, the European Commission found that Microsoft had violated Article 82 of the EU Treaty by abusing its near-monopoly in the market for the Windows operating system. The abuse stemmed both from deliberately limiting interoperability between Windows PCs and non-Microsoft work group servers, and from tying the Windows Media Player to its ubiquitous operating system.

As a remedy focused on restoring interoperability, the Commission required Microsoft, within 120 days, to disclose complete and accurate interface documentation enabling non-Microsoft work group servers to achieve full interoperability with Windows Server and Windows PCs[132]. For the purpose of monitoring Microsoft's compliance with the Decision, a Monitoring Trustee was appointed with the task to assess whether the information made available by Microsoft is complete and accurate, whether the terms under which Microsoft makes the specifications available and permits their use are reasonable and non-discriminatory, and whether the ongoing disclosures are made in a timely manner[133].

One practical issue is worth mentioning here: Microsoft claimed that access to the information necessary to interoperate with its work group server constituted a trade secret, and therefore it could legitimately refuse to disclose it to third-parties who wanted to build dedicated applications. The Commission gave short drift to this argument, forcing the

131 The relevance of this case was stressed by the European Commission's oral response to the Questionnaire.

132 Case COMP/C-3/37.792 — Microsoft. See Press Release, available at: <https://europa.eu/rapid/press-release_IP-04-382_en.htm>. Accessed 30 March 2026.

133 See "6.1.3. Monitoring Mechanism" in Commission Decision of 24.03.2004 relating to a proceeding under Article 82 of the EC Treaty (Case COMP/C-3/37.792 Microsoft) at <https://ec.europa.eu/competition/antitrust/cases/dec_docs/37792/37792_4177_1.pdf>. Accessed 30 March 2026.

company to disclose complete and accurate specifications for the protocols used by Windows work group servers in order to provide file, print and group and user administration services to Windows work group networks. However, in defining the remedy, it made clear that the decision did not contemplate compulsory disclosure of Windows source code, which was arguably the most valuable part of Microsoft´s trade secrets, and that this restriction on Microsoft´s ability to fully enforce any of its intellectual property rights was justified by the need to put an end to the abuse.

Furthermore, to ensure that this restriction remained limited to what was necessary to remedy the abuse and minimize the interference with Microsoft's intellectual property, it provided that specifications should also not be reproduced, adapted, arranged or altered, but merely be used by third parties to write their own specification-compliant interfaces. It is also interesting to note that one aspect of the remedy that permitted to refrain from ordering full disclosure of the code was the expected designation of a trustee to monitor compliance: the Commission ordered Microsoft to submit a proposal for the establishment of a mechanism which is to include a monitoring trustee, at Microsoft´s own cost, "with the power to have access, independently of the Commission, to Microsoft's assistance, information, documents, premises and employees and to the source code of the relevant Microsoft products".

Ultimately, this part of the remedy ended up being annulled on appeal because of the broad and indeterminate order, more specifically on three grounds: (i) it entailed the delegation to the monitoring trustee of powers of investigation which the Commission alone can exercise; (ii) it imposed on the undertaking the costs for fulfilling its own responsibility; and (iii) by imposing the task to act on its own initiative and without time-limits it went "far beyond the situation in which it retains its own external expert to provide advice when it

investigates the implementation of the remedies prescribed in the Decision[134]".

The Decision is also interesting as far as the remuneration for the disclosure of interoperability information is concerned: its "pricing principles" in this regard required the monitoring trustee to examine whether it was Microsoft's own creation, whether it constituted innovation, and take into account the market valuation of comparative technologies excluding the strategic value derived from the dominant position of any such technologies[135].

The **European Commission** has imposed interoperability in a number of occasions aside from the *Microsoft* case discussed above, particularly in merger cases: these include *Qualcomm/ NXP*[136], *Microsoft/LinkedIn*[137], *Broadcom/Brocade*[138], *Intel/ McAfee*[139] , *Daimler/ BMW car sharing JV*[140] and *Google/Fitbit*[141]. While these remedies all concerned mandated interoperability in a similar fashion as the cases discussed so far, more interesting for illustrative purposes is the *Cisco/Tandberg* merger[142], where the Commission approved Cisco´s acquisition of videoconferencing vendor Tandberg subject to a remedy that addressed the concern of future lack of interoperability between Cisco´s products and competing videoconferencing solutions.

The reason why this case differs from others is that the Commission, perhaps weary of the difficulty of monitoring

134 Case T-201/04, *Microsoft v Commission* [2007] ECR II-3601, paragraph 1263-1279.

135 VESTERDORF, B., FOUTOUKAKOS, K., ´An Appraisal of the Remedy in the Commission's Google Search (Shopping) Decision and a Guide to its Interpretation in Light of an Analytical Reading of the Case Law´, 9 (13) Journal of European Competition Law & Practice (2018)

136 Commission Decision of 18 January 2018 *(Case M.8306 -Qualcomm/NXP).*

137 Commission Decision of 6 December 2016 *(Case M.8124- Microsoft/LinkedIn).*

138 Commission Decision of 12 May 2017 *(Case M.8314- Broadcom/Brocade).*

139 Commission Decision of 26 January 2011 *(Case No COMP/M.5984 – Intel/McAffee).*

140 Commission Decision of 7 November 2018 *(Case M.8744- Daimler/BMW car sharing JV).*

141 Commission Decision of 17 December 2020 (Case COMP/M.9660 – *Google/Fitbit*).

142 Commission Decision of 30 March 2010 *(Case No COMP/M.5669 - Cisco/Tandberg).*

compliance with this obligation over time, did not simply impose the duty on Cisco to ensure interoperability for a specified period: rather, it required Cisco to divest the copyright of the TIP (Telepresence Interoperability) protocol[143], which Cisco had already offered for license to competitors in order to guarantee interoperability between Cisco and non-Cisco endpoints. Also, it required, within 120 days of closure of the transaction, to assign the responsibility for managing and updating it to a third-party: either the International Multimedia Telecommunications Consortium or (in case the latter refuses) to an independent industry body which fulfills certain conditions[144]. Further, to facilitate the task of this body and prevent "forking", Cisco also committed not only to publish an open-source library with information about the development of the current version of TIP, but also, to participate in the open-source development efforts by the independent industry body, implement and support TIP on its existing and future products.

All in all, this remedy package, in particular the set of provisions that are designed to ensure impartiality and openness of the independent industry body, traces an alternative path for interoperability. This is in line with the proposal that the definition of interoperability standards ought to be set by a technical committee, overseen by the antitrust enforcer, as it would allow representation of all interests and avoid the extreme positions of a defendant and the authority or

143 See Cisco, 'Telepresence Interoperability Protocol for Developers' (2019), Available at <https://community.cisco.com/t5/%E5%8D%8F%E4%BD%9C%E5%8D%9A%E5%AE%A2/telepresence-interoperability-protocol-for-developers/ba-p/4383759>. Accessed 30 March 2026: "Opened up Telepresence Interoperability Protocol (TIP). Cisco has opened up and transferred its Telepresence Interoperability Protocol (TIP) to the International Multimedia Telecommunications Consortium (IMTC) to license royalty-free to anyone. Those wanting a multi-stream interoperability option with Cisco now can implement TIP as well as participate in its ongoing stewardship as a member of IMTC."

144 Namely, procedures are transparent, members have equal voting rights, decisions regarding the finalization of revisions to TIP would be based on the consensus views of members, and all information necessary to apply the TIP Protocol and Implementation Profiles will be made available for those who wish to enter the market.

plaintiff[145]. These proponents also warn that the remedy must include provisions that will deter the defendant from violating the order, require standards that many entrants can meet, and not favor large incumbents, and have a speedy process to determine whether the remedy order has been violated.

A more recent merger decision involving interoperability as a remedy is **Meta/Kustomer**[146]. As per the European Commission's assessment, Kustomer was an innovative and fast-growing player in the customer service and support customer relationship management ("CRM") software market, and Meta´s messaging applications constitute inputs for customer service and support CRM software providers. The Commission found that Meta would have both the ability and the incentive to foreclose Kustomer's rivals – for example, by denying or degrading access to the APIs for Meta's messaging channels. Since these competitors have a focus on small and medium business customers ('SMBs'), such foreclosure could reduce competition in CRM and customer service CRM markets, leading to higher prices, lower quality, and less innovation for business customers, especially SMBs, with possible negative effects on consumers.

Meta submitted a two-fold commitment for a ten-year term, which was considered sufficient to address the foreclosure concerns: first, to guarantee non-discriminatory access, without charge to its publicly available APIs for its messaging channels to competing customer service CRM software providers and new entrants; second, to make available any eventual improved or updated features or functionalities of Messenger, Instagram messaging or WhatsApp that are currently used by Kustomer's customers, or any new such

145 SCOTT MORTON, F. KADES, M., ´Interoperability as a Competition Remedy in Digital Networks´ (March 19, 2021). Available at SSRN: <https://ssrn.com/abstract=3808372> or <http://dx.doi.org/10.2139/ssrn.3808372>. Accessed 30 March 2026.

146 European Commission, 'Mergers: Commission clears acquisition of Kustomer by Meta (formerly Facebook), subject to conditions'´, Press Release (30 January 2022) at <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_652>. Accessed 30 March 2026.

features that are used by a sizeable proportion of Kustomer's customers. For our purposes, it is noteworthy that the remedy carefully distinguishes between publicly available and private API, requiring Meta to grant access to it without charge for competing messaging channels, but also publish details of relevant APIs and functionalities on its website.

The Commission relied on the appointment of a monitoring trustee to oversee the remedy implementation, with powers to access Meta's records, personnel, facilities or technical information, and to appoint a technical expert to assist in the performance of its duties. Compared to Microsoft, the remedy foreshadowed possible disagreements with third parties in the implementation by including a fast track and binding dispute resolution mechanism, a feature that is recommended in the latest EU Remedy Notice[147] to avoid the need for permanent monitoring by the Commission, if effective and timely (para 66), and can be observed in many recent trustee mandates. Also, with a view to preserving trade secrets and commercially valuable information, it explicitly provides for the trustee´s duty of confidentiality (which was surprisingly absent from the requirements identified in the Microsoft remedy) *vis a vis* any third party other than the Commission and any appointed technical expert. This revised approach to confidentiality is in line with the added concern, in the EU Remedy Notice, for the transmission to licensors of sensitive information concerning the competitive behavior of the licensees which are active as competitors in the downstream market, (e.g., the number of licenses used in that market), which must be addressed in order for a commitment to be suitable (para. 65).

More recently, the **European Commission** imposed interoperability as a remedy in the **Apple Pay** case[148],

147 EUROPEAN COMMISSION (2008), Notice on remedies acceptable under Council Regulation (EC) No 139/2004 and under Commission Regulation (EC) No 802/2004 (Text with EEA relevance), OJ C 267, 22.10.2008, p. 1–27

148 The relevance of this case was stressed by the authority in response to the Questionnaire.

concerning Apple's mobile wallet used to allow iPhone users to pay with their devices. According to the Commission's preliminary investigation, Apple abused its dominant position by refusing to grant rivals access to the standard technology used for contactless payments with iPhone in stores – Near-Field-Communication (NFC) or "tap and go" – while reserving this access only to Apple Pay.

Apple offered commitments that involved, among other things, allowing third-party wallet providers access to the NFC input on iOS devices free of charge, without having to use Apple Pay or Apple Wallet. Specifically, Apple would enable access to NFC in Host Card Emulation mode ('HCE'), which allows to securely store payment credentials and complete transactions using NFC without relying on an in-device secure element. The remedy package also included (i) enabling users to easily set an HCE payment app as their default app for payments in stores and to use relevant functionalities; (ii) using fair, objective, transparent and non-discriminatory procedure and eligibility criteria to grant NFC access to third-party mobile wallet app developers; and (iii) a monitoring mechanism and separate dispute settlement system to allow for independent review of Apple's decisions restricting access. After market testing the commitments proposed by Apple, the Commission concluded that Apple's final commitments version would address its competition concerns, because they open up competition in mobile payments on iPhone[149].

We can also find useful inspiration from the decision taken by the **European Commission** in March 2025 involving **Apple** and its compliance with article 6 (7) of the Digital Markets Act, which requires gatekeepers to allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the

149 European Commission. 'Commission accepts commitments by Apple opening access to 'tap and go' technology on iPhones (Press Release, Jul. 10, 2024) Available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3706>. Accessed 30 March 2026.

same hardware and software features accessed or controlled via the operating system or virtual assistant as are available to services or hardware provided by the gatekeeper. It should be noted that this duty is subject to the provison that the gatekeeper shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, to the extent this is duly justified.

In March 2025, the European Commission adopted a so-called implementation decision, which specifies the detailed measures Apple must take to comply with that provision. It is notable that the Commission addresses the scope of the "integrity" exception to clarify that it is strictly limited to protecting the correct functioning of the operating system and its features from being impaired or corrupted, therefore not allowing Apple to impose its own model of security and privacy on third parties or to deny access simply because a third party is not Apple[150]: every restriction to interoperability must be "strictly necessary and proportionate" to address a specific, genuine integrity risk.

The Commission rejected Apple's narrow interpretation that the obligation would only be in favor of actual competitors (as opposed to any interested third parties), explaining that the DMA is about protecting innovation, and therefore benefitting all providers of services and hardware. It also clarifies that the obligation should be future-proof, applying to new features that Apple develops, and that any interoperability solution being available to all developers in equally effective manner (including proper documentation).

It provides some important guidance in terms of transparency, requiring that Apple makes available a clear public webpage with detailed guidance on the process and a reliable contact

150 Recitals 80-95

point which provides regular, detailed status updates to developers that have submitted an interoperability request. Such requests must be dealt with under a predetermined timeline (longer where more complexity is involved) and preserve the confidential information of developers from being used by competing business units at Apple. Furthermore, any rejection must be accompanied by detailed reasoning and guidance on how to challenge it, first through an internal review process and subsequently, if necessary, through conciliation with an independent technical expert with reasonable costs (covered by Apple in case of SMEs). Apple must also publish KPIs regarding its requests, timelines, rejections, and dispute resolutions. This framework provides a useful roadmap of the issues that must be considered when drafting interoperability mandates.

(iii) Data Segregation

Definition

Data segregation is a concept that is not legally defined and is often used interchangeably with the term "data silos". However, technically speaking, there appears to be a notable difference between the two. According to the Oxford Learner's Dictionaries, "segregation" refers to "the act of separating people or things from a larger group", whereas "silo" is a system, process, department, etc. that "operates separately or is thought of as separate from others"[151]. From these definitions, it is apparent that segregation refers to a deliberate act of separation, whereas silo may be the result of a broader set of actions, including deliberate acts but also unintended or non-purposeful system construction.

When bringing these terms to the realm of remedies, however, one can rule out the lack of intentionality, insofar as both types would describe the way in which a firm must implement the prohibition to use certain data for a particular purpose. Nevertheless, the degree of specificity

151 See <https://www.oxfordlearnersdictionaries.com/definition/english/segregation> Accessed 30 March 2026.

to which said principle is crafted may vary, potentially encompassing also the need for segregation. In accordance with this, for purposes of this Report, it is suggested that data segregation constitutes a special category of the remedy called "data use prohibition". This is because data segregation requires the creation of an infrastructure that ensures the separate processing of two or more datasets, whereas data use prohibition may simply impose a limitation on the use of one dataset. Data segregation will typically include prohibitions to export and/or combine the relevant data with others, but the remedy order may go beyond that: it often prescribes the creation of a vertical firewall within the company in question.

Vertical firewalls involve the restriction of transfers of information from one business or asset of the company to another[152], and therefore may be considered as remedies in cases involving the leveraging of valuable information. While appropriate in principle, these measures raise doubts in terms of implementation and oversight. Contacts and exchanges of information are quite common within the same corporate group[153], casting doubt on the ability of an authority (or even a third party, such as monitoring trustee) to verify compliance.

Since doing this would require continued control over the merged entity, the German authority does not consider this a suitable remedy[154], in line with the interpretation given in a court case on the matter[155]. Other authorities[156] recognize that the asymmetry of information over the behavior of merging parties compromises the effectiveness of this remedy. However, they find this measure more effective when imposed

152 This may involve a range of restrictions in information flows and use of shared services, physically separating premises and staff, and regulating transfers of management and any permitted interactions between relevant staff. See CMA´s Guide on Merger Remedies (CMA, 2018), para. 7.25.

153 BUNDESKARTELLAMT, Guidance on Remedies in Merger Control (2017) at <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitlinien/Guidance%20on%20Remedies%20in%20Merger%20Control.pdf?__blob=publicationFile&v=4> Accessed 30 March 2026.

154 Id.

155 BundesKartellAmt Decision of 27.10.2005, B6-86/05 – PVN/Buch und Presse/MSV.

156 For instance, see the merger remedies guide released in 2018 by the CMA (see <https://assets.publishing.service.gov.uk/media/5c12349c40f0b60bbee0d7be/Merger_remedies_guidance.pdf>) and CADE (see <https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/Guide-Antitrust-Remedies.pdf>). Accessed 30 March 2026.

together with other remedies[157] and when parties commit significant resources to educating staff about the requirements of the measures and supporting them with disciplinary procedures and independent monitoring[158].

Application

Canada

An early application of this remedy is the case brought by the **Canadian competition authority** in **McKesson Canada Corporation and Rexall Pharmacy Group Ltd**[159], from 2016, as indicated in the authority's response to the questionnaire. Here, a consent agreement was entered into to address concerns arising from McKesson's proposed acquisition of the healthcare businesses of the Katz Group, which included the Rexall pharmacy retail chain and the ClaimSecure healthcare claims adjudication business. The Katz Group's Rexall chain was among the largest retailers of pharmaceutical products in Canada and the ClaimSecure was a health-care claims adjudication provider that connected to 99% of all licensed pharmacies in Canada and processed more than 10 million health and dental benefit transactions annually on behalf of corporations, insurers, unions, and other plan sponsors representing approximately 1.2 million Canadians.

To mitigate the competition concerns identified, the consent agreement required McKesson to divest Rexall retail locations in 26 local markets across Canada. It further established a set of firewalls restricting the transmission of commercially sensitive information among McKesson's wholesale operations, the Rexall retail business, and the ClaimSecure adjudication business. The consent agreement defined specific categories of confidential

157 CADE, id.

158 CMA, id.

159 See <https://competition-bureau.canada.ca/en/acquisition-katz-groups-healthcare--mckesson>. Accessed 30 March 2026.

information and mandated that each category be kept strictly confidential and not used outside its respective business unit. For example, ClaimSecure Confidential Information[160] could be used solely for the operation of the ClaimSecure Business and was prohibited from being used in connection with either the Wholesale Business or the Retail Business[161].

Another merger brought by the **Canadian competition authority,** indicated in their answer to the questionnaire, that involved the imposition of segregation remedies was **The Coca-Cola Company's (TCCC[162]*)* acquisition of** the North American carbonated soft drink business of its primary bottler, **Coca-Cola Enterprises Inc. (CCE)**. Prior to the proposed transaction, CCE produced, marketed, and distributed not only Coca-Cola products but also beverages for Dr Pepper Snapple Group, Inc. The Competition Bureau concluded that the proposed acquisition could allow The Coca-Cola Company to gain access to the marketing plans and other commercially sensitive information of Canada Dry Mott's Inc. (CDMI), a subsidiary of Dr Pepper Snapple Group, Inc., and would therefore be likely to substantially lessen and/or prevent competition in the supply of soft drinks in Canada.

A consent agreement was adopted to address these competition vertical concerns. The firewall remedy effectively partitioned the flow of information between two downstream rivals (Coca-Cola and CDMI) after the vertical integration of one of them (Coca-Cola) with its supplier. The firewalls

160 "ClaimSecure Confidential Information' means all transaction data provided to or generated by ClaimSecure for the purposes of dispensing patient prescriptions, determining patient eligibility under drug benefit plans, or adjudicating and processing drug benefit claims, including the final selling price of all prescription drug reimbursements processed by the ClaimSecure Business, that is not in the public domain, except that ClaimSecure Confidential Information shall not include aggregated data in a de-identified format that ClaimSecure sells or makes available to Third Parties generally" see section 1(h) of the Consent Agreement. Available at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/462949/index.do>. Accessed 30 March 2026.

161 McKesson Canada Corporation and Rexall Pharmacy Group Ltd. Registered Consent Agreement (14 Dec. 2016) at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/462949/index.do>. Accessed 30 March 2026.

162 Coca-Cola. Registered Consent Agreement (27 Sept. 2019) at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/463530/index.do>. Accessed 30 March 2026.

restrict both the use of and access to CDMI's commercially sensitive information, including limitations on access to relevant personnel. Moreover, CDMI's commercially sensitive information could be used solely for the purpose of bottling and distributing CDMI beverages.

Finally, another relevant decision by the **Canadian competition authority** is the **acquisition by BCE Inc. and Rogers Communications Inc. of a 50% stake each in Glentel Inc**., which entailed the imposition of data segregation remedies[163]. BCE and Rogers are both telecommunications service providers, while Glentel operated wireless retail stores.

In this case, the 2025 consent agreement required the implementation of administrative firewalls between BCE, Rogers, and Glentel to prevent the sharing of competitively sensitive information, including subscriber data, pricing, and promotional offers. Specifically, the consent agreement required each of BCE and Rogers to (i) maintain exclusive and independent control over, and management of, their respective promotional and marketing plans; (ii) remain responsible for their own sales efforts; (iii) maintain complete and unrestricted discretion to establish their end-user pricing; and (iv) not exchange any information regarding pricing, promotions, or marketing plans with the other shareholder.

European Union

In the European Union, a recent remedy involving a commitment for the acquirer not to use certain data is the one adopted by the **European Commission** in **Google/ Fitbit**[164]. After assessing the case, the Commission understood that there was a horizontal competition risk, not because the parties

163 BCE Inc. and Rogers. Registered Consent Agreement (5 May 2015) at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/463122/index.do>. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

164 Commission Decision of 17 December 2020 (Case COMP/M.9660 – *Google/Fitbit*).

operate in the same market, but because the acquisition would combine two sets of inputs, Google's data and Fitbit's data.

The Commission's decision, applying the Horizontal Merger Guidelines, explains that this combination of data could hinder the entry or expansion of competitors, as Google would control a vast amount of user data – from emails and date of birth to weight, sleep, water intake, etc. Data control would strengthen the company's dominant position in the online advertising market. Therefore, the specific part of the remedy that imposed a duty on the acquirer not to use certain data was designed to address Google´s strengthening of market power in online advertising with the acquisition of Fitbit, a producer and distributor of wearable devices, software and services in the health and fitness sector. Google committed to maintain a separation between Fitbit data and Google's advertising systems data into *data silos*, ensuring that Fitbit health data would not be used for targeted advertising purposes.

Before taking a decision in this case, the Commission consulted both the European Data Protection Board (the advisory body comprising data protection authorities of EU Member States) and the European Data Protection Supervisor (the authority in charge of data protection for EU institutions)[165]. It is not clear if it is because of their input, but it is notable that, after market testing, the Commission went beyond its original scope: it clarified that the commitment not to use Fitbit customer data for 10 years extended not only to personally identified or identifiable data of Fitbit´s customers, but also to any inference, modification or derivation of such data, including after the use of techniques of anonymization, pseudo-anonymization, de-anonymization or aggregation.

In 2022, the **European Commission** accepted commitments offered by **Amazon** involving a data segregation remedy[166]. This

165 OECD DAF/COMP/WD(2024)30. The intersection between competition and data privacy – Note by the European Union.

166 See <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777>. The rele-

marked the closing of an investigation into Amazon's practice (among others) to access and use non-publicly available data relating to third-party sellers' listings and transactions, that Amazon obtains in the context of its marketplace services, for the purposes of Amazon's own retail operations in competition with those sellers. Under the data-silo commitment, Amazon commits itself not to use non-public data[167] provided by third-party sellers to Amazon in the context of their use of Amazon's marketplaces services, or derived through third-party sellers' use of Amazon marketplace services or related services such as payment and fulfilment services, for the purposes of Amazon's own retail operations, in competition with those third-party sellers. In particular, Amazon commits itself not to use such third-party seller data either via Amazon's automated systems or via its employees, whether for the purposes of selling branded goods or for the purposes of selling its private label products. The relevant data covers aggregated, individual, anonymized and personal data, whether in raw form or processed.

Japan

The **acquisition of Fitbit by Google** was also examined by the **Japanese competition authority** in 2021[168], as indicated by JFTC in response to the questionnaire. Although the transaction did not meet the notification thresholds set out in the Antimonopoly Act, the overall consideration for the acquisition was substantial and was expected to have implications for domestic consumers; the JFTC therefore proceeded to review the transaction. The authority ultimately concluded that the remedies offered by the parties to address

vance of this case was highlighted by the authority in its oral response to the Questionnaire.

167 Meaning "data not made available to Sellers by Amazon or otherwise available through published sources (including the Amazon Store)". Cf. <https://ec.europa.eu/competition/antitrust/cases1/202252/AT_40462_8825091_8265_4.pdf>. Accessed 30 March 2026.

168 Japan Fair Trade Commission (JFTC), Press Release. 'The JFTC Reviewed the Proposed Acquisition of Fitbit, Inc. by Google LLC' (14 January 2021) at <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114.html>. Accessed 30 March 2026.

competition concerns related to the use of data for advertising purposes were sufficient to approve the acquisition subject to those offers. With respect to data-related issues, Google committed (i) not to use certain health-related data (i.e. physical measurement data and health and fitness activity location data) in its digital advertising-related business, and (ii) to maintain the separation of such health-related data from other datasets within Google. Google was required to adhere to both commitments for a period of ten years from the date of the acquisition, with the possibility of an extension of up to an additional ten years[169].

South Africa

In South Africa, a similar decision was taken on **Google/Fitbit** in 2020. The **Competition Commission of South Africa** found that the proposed merger was likely to result in a substantial prevention or lessening of competition. The concerning was that as a result of the proposed merger, Google could: (i) exclude Fitbit's competitors in the market for wrist-worn wearable devices, (ii) entrench its dominance in the online advertising and online search market and (iii) restrict access to health data collected by Fitbit, excluding other players or potential entrants in the digital health market or other health services markets.

Google committed to comply for ten years with the following: (i) to make "access to the Android OS available, without charge for entry and on a non-discriminatory basis, under the same license terms and conditions that currently apply, to all competing manufacturers of wrist-worn wearable devices"[170]; (ii) to maintain data segregation between the Fitbit

169 Japan Fair Trade Commission (JFTC), 'The JFTC's Review Results concerning Acquisition of Fitbit, Inc. by Google LLC (January 2021) at <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114r.pdf>, p. 28. Accessed 30 March 2026.

170 BRICS Competition Centre, 'South African Competition Commission conditionally approves the Google/Fitbit merger' (23 December 2020) at <https://www.bricscompetition.org/news/south-african-competition-commission-conditionally-approves-the-googlefitbit-

data and Google's existing data and not using any measured body data or health and fitness activity location data from Fitbit for Google Ads; and (iii) to offer each South African user the choice to grant or deny use by Other Google Services (excluding Google Ads) of any Measured Body Data stored in their Google or Fitbit account. Regarding API conditions, Google also committed "to allow third parties that currently access Fitbit's data to continue to have access to users' health and fitness data through the Fitbit Web API, without charging for access and subject to user consent"[171].

United Kingdom

Similarly to the aforementioned European Commission case, in **United Kingdom, the CMA** investigated[172] some **Amazon** practices regarding the access and use of non-publicly available data relating to third-party sellers' listings and transactions, that Amazon obtains in the context of its marketplace services, for the purposes of Amazon's own retail operations in competition with those sellers. At the end of the investigation, the CMA accepted the company's commitments aimed to

> (i) ensure that Amazon does not use marketplace data from competing sellers to gain an unfair advantage;
>
> (ii) ensure that all product offers are treated equally when Amazon decides which ones will appear in the Buy Box; and
>
> (iii) allow third-party businesses using the marketplace to negotiate their own rates directly with independent

-merger>. Accessed 30 March 2026.

171 Competition Commission of South Africa, 'Competition Commission conditionally approves the Google/Fitbit merger' (Media Statement, 22 December 2020) p. 4 at <https://www.compcom.co.za/wp-content/uploads/2020/12/Competition-Commission-conditionally--approves-the-Google-Fitbit-merger.pdf>. Accessed 30 March 2026.

172 Competition and Markets Authority (CMA), 'Investigation into Amazon's Marketplace' (6 July 2022, last updated 12 February 2024) at <https://www.gov.uk/cma-cases/investigation--into-amazons-marketplace>. Accessed 30 March 2026.

providers of Prime delivery services, so that customers can benefit from lower delivery costs when better rates are obtained.

Croatia

The **Croatian competition authority** also applied a data segregation remedy in 2022, in a merger case concerning the **acquisition of direct control over Renault Nissan by Grand Automotive LLP and Grand Automotive RD Ltd**[173]. As a condition for approving the transaction, the authority imposed several measures to mitigate potential anticompetitive effects. Among these measures, Grand Automotive LLP committed to amend the information-business system used by Hyundai Hrvatska d.o.o. and by the authorized repairers and/or distributors within the Hyundai Hrvatska sales and service network, as well as the system used by Grand Dalewest d.o.o. and the authorized repairers and/or distributors in the Ford sales and service network, so as to prevent access to and the flow of competitively sensitive information and data (particularly inventory information, vehicle sales data, and financial data) between individual members of the authorized Hyundai and Ford sales and service networks. This excluded the exchange of data relating to the service and repair history of individual vehicles, warranty recording, processing and monitoring, and the search and retrieval of vehicle-specific data by VIN.

The measures also included preventing any authorized Ford or Hyundai repairer/distributor from accessing competitively sensitive information and data visible to another authorized Ford or Hyundai repairer/distributor, regardless of any potential consent between the network members. In addition, Grand Automotive LLP was required to amend the existing

173 Croatian Competition Authority, 'Case No UP/I 034-03/2022-02/005, URBROJ 580-11/107-2022-052', Conditionally Approved Concentration (Zagreb, 9 August 2022) at <https://www.aztn.hr/ea/wp-content/uploads//2023/03/UPI-034-032022-02005.pdf>. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

information-business system used by Renault Nissan Hrvatska d.o.o. so that, with respect to the flow of information and competitively sensitive data between members of the authorized Renault, Nissan and Dacia distribution-service network and Renault Nissan Hrvatska d.o.o., as well as among the network members themselves, the system fully complies with the information-segregation mechanisms set out in the decision.

Hungary

The **Hungarian competition authority** (GVH) also imposed, in 2024, this type of remedy in a merger case concerning the **acquisition of iLogistic** – a company dedicated to fulfillment activities – **by General Logistics Systems B.V**., a member of the GLS Group, mainly active in the logistics sector[174]. The remedy took the form of a "Chinese Wall" in order to ensure data segregation.

Specifically, GLS Hungary (the Hungarian member of the GLS Group), and General Logistics Systems B.V., the notifying party, were required to implement a structural and functional separation between iLogistic (the target company providing fulfillment services), and GLS Hungary (the acquirer's Hungarian parcel delivery subsidiary). In particular, GLS Hungary was prohibited from accessing commercially sensitive data belonging to competing parcel delivery companies that had been disclosed to iLogistic during business negotiations (e.g., pricing terms, commercial offers). To this end, a "Chinese Wall"-type commitment was required to ensure the creation of internal safeguards within iLogistic, including (i) independent

174 Gazdasági Versenyhivatal – GVH (Hungarian Competition Authority), VJ/32/2022 (Budapest, 10 April 2024). The relevance of this case was highlighted by the authority in its response to the Questionnaire. at <https://www.gvh.hu/pfile/file?path=/dontesek/versenyhivatali_dontesek/versenyhivatali_dontesek/dontesek-2022/Vj032_2022_m.pdf1&inline=true>. Accessed 30 March 2026.

decision-making structures, (ii) isolation of key data flows and access and (iii) the prevention of undue influence by GLS-appointed executives over processes involving competitors' relevant data.

In its assessment, the case team also considered compliance with data protection rules, particularly GDPR principles, as well as those set out in the relevant Hungarian legislation, such as purpose limitation and data minimization. The GVH emphasized that all data exchange between fulfillment providers and clients (including parcel carriers) must comply with the principle of purpose limitation. Accordingly, the remedy explicitly sought to prevent misuse of such data by prohibiting any cross-access of competitively sensitive information, ensuring that GLS Hungary would have no access to data obtained by iLogistic from other parcel delivery firms, and addressing market concerns about profiling or competitive targeting through improper data use.

(iv) Data access/sharing

Definition

Data sharing is a comprehensive term that is typically used in the remedy context to imply an economic operator (typically, a competitor) getting some level of access to a firm's dataset. Access remedies imply an obligation to grant access to key infrastructure, networks, technology and essential inputs.

Due to the significant interference with a company´s property rights, great caution is advised when deciding to impose this type of remedy, as it can undermine the incentives to build the shareable asset. This requires an authority to balance the short-term effects of the remedy with the long-term effects on investment.

The need for *ex post* appropriability is not invariably strong, with one example in the opposite sense being when the facility has been created through public funding or is protected by weak intellectual property

rights[175]. One could also argue that such need is also not very strong when it comes to data, if this is a byproduct of a company's operation and not a key asset to guarantee returns on investment. Therefore, it can be argued that the balancing of the benefits of access against those of closure should weigh more heavily towards the former.

When warranted, mandated access may serve both the preventative purpose of addressing leveraging concerns, and the restorative aim of facilitating entry by competitors. It is common to request that such access be provided on (fair) reasonable and non-discriminatory (FRAND) conditions, and since how those qualifications are to be interpreted and enforced in a particular case is a matter typically resolved through court or arbitration, this kind of remedy usually includes provisions for such mechanisms. Alternatively, a remedy may grant competitors free access, as occurred in the *Google/Fitbit* merger decision with regard both to the fitness data (subject to consumer consent) and the Application Program Interfaces containing the information needed for interoperability between the Android ecosystem and competing wrist-wearable devices.

When defining the boundaries of data access, a *first* difficulty may concern the scope of the obligation. Access to a large dataset is deemed unlikely to be necessary if only a specific subset of such data is needed to allow competition in-the-market to unfold. However, determining the appropriate scope and level of granularity may be challenging. For instance, would the selection be based on the basis of the sector in which the undertaking operates? On the basis of the number of data points for each individual in the dataset? On the basis of the commercial value of such data or its availability from other sources in the market? We do not intend to answer those questions but only highlight them to allow further discussions.

A *second* challenge is the interaction of the remedy with data privacy considerations. In particular, concerns may arise if the data to which access is being sought are of personal nature, as it implies that the

175 Ashwin Van Rooijen, The Role of Investments in Refusals to Deal, 31 World Competition 63 (2008)

sharing of such data would need to comply with the applicable data protection rules, including being grounded on a lawful legal basis. For this reason, the involvement of a data protection authority in crafting the terms of the remedy may be necessary or at least recommended.

One seemingly intuitive way to align the remedy with data protection law is to condition the sharing upon the consent of the data subjects. In this case, the sharing would replicate the dynamics of banking and financial services with the rise of Open Banking. However, the details of what constitutes a valid consent can be controversial. For instance, it may be that a mere opt-out does not suffice. In this sense, it is said that the GDPR imposes a "high bar" when establishing that "when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract"[176] and that "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller"[177], both of which may jeopardize the validity of consent in the context of a standardized mass contract.

An alternative legal basis for the processing of personal data may be compliance with a legal obligation, which would be the remedy itself[178]; however, this solution does not cover the further processing by the beneficiaries of the data, leaving a potential gap which might frustrate its effectiveness.

Finally, a *third* option usually given is the reliance on the legitimate interest[179], both of the controller (in not being subject to a fine) and of third

176 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, art 7 (4).

177 Ibid., recital 43.

178 KATHURIA, V., GLOBOCNIK, J., ´Exclusionary conduct in data-driven markets: limitations of data sharing remedy´, Journal of Antitrust Enforcement, Volume 8, Issue 3, November 2020, Pages 511–534.

179 However, this legal basis is not available for the processing of "special categories" of data, such as those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person's sex life or sexual orientation. See art. 9 (1) of the GDPR.

parties (to benefit from a more competitive environment). This, however, may not be sufficient to outweigh the interest and fundamental rights of the data subjects not to have their data duplicated and distributed to competitors[180]. Nonetheless, this legal basis may be suitable if the data controller adopts safeguards for data subjects' rights and interests, such as the use of anonymization or pseudonymization techniques, providing additional notice(s) and consent, an unconditional right to opt-out, increased transparency, expanded data portability, and avoiding use of research data for actions about individual[181].

An academic study suggested a design feature for the remedy which could make the legitimate interest basis more viable, which is create a regulatory sandbox aimed to grant access not to all competitors, but only those who commit to a particular data use: this particular design feature of the remedy could be used to ensure both its competitive relevance and its compliance with data protection principles[182]. In the most extreme cases, access could be granted only *in situ*, in other words accommodating queries for such data within the dataset of the original contributor, which has the advantage of preserving the contextual elements that enhance the value of the data in question[183].

Application

Canada

A case from the **Canadian competition authority** in the 1990s provides useful guidance for understanding this type

180 GRAEF, I. THOMBAL, T., DE STREEL, A., 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' Background Note for the meeting of the Digital Clearinghouse of 19 November 2019, available at <https://static1.squarespace.com/static/5cb4d40365a7070cc7d2d1fc/t/5ddf946ee6b0e7013a3622d7/1574933616451/DCH+-+Background+note+Final+website.pdf>. Accessed 30 March 2026.

181 ARTICLE 29 WORKING PARTY, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (14 April 2014), at <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Accessed 30 March 2026.

182 ZINGALES, N., Data Collaboratives, Competition Law and the Governance of EU Data Spaces (July 31, 2021). Forthcoming in KOKKORIS, I. (ed.), *Research Handbook in Competition Enforcement* (Edward Elgar, forthcoming 2022).

183 PARKER, G., PETROPOULOS, G., VAN ALSTYNE, M. W., ´Platform Mergers and Antitrust´,
30 (5) *Industrial and Corporate Change* (October 2021), 1307–1336.

of remedy[184]. In 1994, **D&B Companies of Canada Ltd.** was investigated for abuse of dominant position under section 79 of the Competition Act. The company, which substantially controlled the supply of scanner-based market tracking services in Canada, was alleged to have entered into exclusive contracts for scanner data with retailers, offered significant financial incentives to secure exclusive access to their scanner data, and concluded long-term agreements with manufacturers of consumer-packaged goods to provide market tracking services, imposing penalties for early termination[185].

As a result, D&B was required by the Competition Bureau, for a period of nine months from the date of the Order – upon request of a supplier (or potential supplier) of a scanner-based market tracking service, and if so directed by a supplier of retailer scanner data that had not retained its own historical scanner data – to provide historical scanner data covering a period of fifteen months prior to the request. The Order also set out the applicable fees for providing such data.

While this remedy did establish an option for data sharing upon the request of a supplier or potential supplier of a scanner-based market tracking service, most of the provisions in the remedy imposed prohibitions on certain conduct rather than prescribing to whom the data should be made available. For example, the Order imposed a prohibition on D&B from entering into contracts that preclude or restrict a supplier of retailer scanner data from providing a supplier or potential supplier of a scanner-based market tracking service with access to scanner data or causal data necessary for the provision of that service; from offering any inducement to a supplier of retailer scanner data to restrict access by a supplier or potential supplier of a scanner-based market tracking service to scanner data or

184 The relevance of this case was highlighted by the authority in its response to the Questionnaire.

185 D&B Companies of Canada Ltd, Notice of Application (5 April 1994) at https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/464974/index.do.

causal data necessary for the provision of that service, etc[186].

Another important case in the real estate sector was decided by the **Canadian competition authority** in relation to a practice of the **Toronto Real Estate Board** ("TREB") - a trade organization composed of more than 30,000 real estate brokers and salespersons (collectively, "brokers")[187]. TREB is the owner and operator of an electronic database known as the TREB Multiple Listing Service system ("TREB MLS"), which contains current and historical information on the purchase and sale of residential real estate in the Greater Toronto Area (GTA). The TREB MLS is an essential input for the provision of residential real estate brokerage services, as it offers a complete inventory of active and historical listings. However, only TREB members have direct access to it.

According to the investigation, TREB used its control over this system to establish and interpret rules, policies, and agreements with exclusionary and restrictive effects on brokers' access to and use of the TREB MLS. For example, TREB prevents innovative brokers from using secure, password-protected "virtual office websites" (VOWs) to deliver brokerage services online. Allowing VOWs with search functions would enable customers to independently access relevant information on home purchases and sales in the GTA, without relying on the direct assistance of a broker. Brokers and their staff must otherwise obtain such information from the TREB MLS themselves and manually provide it to clients[188].

In June 2016, the Competition Tribunal issued an Order requiring TREB, as a remedy, to include certain "Disputed Data" and information (the "Information") related to real estate listings in its virtual office website (VOW) data feed.

186 D&B Companies of Canada Ltd., Order (Competition Tribunal, 30 August 1995) at https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/464906/index.do.

187 The relevance of this case was highlighted by the authority in its response to the Questionnaire.

188 The Toronto Real Estate Board. Notice of Application (27 May 2011) at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/463477/index.do>. Accessed 30 March 2026.

The competition authority also imposed prohibitive remedies to prevent TREB from precluding or restricting its members' use of the Information in the VOW data feed on any device, and from precluding or restricting its members from displaying on their VOWs, on any device, the Information[189].

Interestingly, the remedy incorporated specific limitations on the use and disclosure of data for privacy-related reasons: (i) TREB may restrict members' use of the Information in the VOW data feed to purposes directly related to the provision of residential real estate brokerage services; (ii) TREB may also prohibit the display on a VOW of a listing or property address where a seller has expressly instructed the listing brokerage to withhold that information from internet display; and (iii) TREB may bar the display on a VOW of the seller's name, as well as remarks or instructions intended solely for members, including security information, access instructions, details regarding when the home will be occupied or vacant, the seller's mortgage information, and other personal information concerning the seller or the home's residents[190].

European Union

Another early scenario involving data sharing, this time as an interim measure, was the **European Commission**'s case, involving **IMS Health** – a global leader in the collection of pharmaceutical sales and prescription data[191]. In 2001, the European Commission found that the company had engaged in abusive conduct by refusing to grant a copyright license for the "1860 brick structure" – a segmentation of Germany

189 The Toronto Real Estate Board. Order (3 June 2016) at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/462955/index.do>. Accessed 30 March 2026.

190 The Toronto Real Estate Board. Order (3 June 2016) at <https://decisions.ct-tc.gc.ca/ct-tc/cdo/en/item/462955/index.do>. Accessed 30 March 2026.

191 European Commission, 'Antitrust: Commission imposes interim measures on IMS Health' (Press Release, 3 July 2003) at <https://ec.europa.eu/commission/presscorner/detail/en/ip_03_1159>. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

into 1860 geographical areas used to report sales data – to its competitor NDC Health.

The 1860 brick structure was considered indispensable for operating in the relevant market, as no actual or potential substitute existed. The Commission therefore adopted a decision on 3 July 2001 ordering IMS, by way of interim measures, to license the 1860 brick structure to its competitors in the market for German regional pharmaceutical sales data services[192]. In this case, the data that was the object of the remedy was not personal, so there was no need to coordinate with the data protection authority.

A second important case decided by **European Commission** occurred in 2007, when four decisions adopted against the car manufacturers **Daimler Chrysler, Toyota, General Motors and Fiat**[193] obliged them to provide technical information on vehicle repairs to all independent garages in the EU.

According to the European Commission, independent repairers play a key role for European consumers, as they exert competitive pressure on authorized dealer networks in the motor vehicle repair and maintenance markets. The investigations found that the manufacturers had withheld certain technical information from independent repairers and had supplied the remaining information in a manner that did not meet their specific needs. As a result of the decisions, the four companies were bound by largely similar commitments, obliging them to make available to independent repairers—in a non-discriminatory manner—the same information provided to authorized repairers, and to ensure that independent repairers can obtain disaggregated information at prices reflecting the

192 European Commission, 'Commission Decision of 3 July 2001 relating to a proceeding pursuant to Article 82 of the EC Treaty '(Case COMP D3/38.044 — NDC Health/IMS Health: Interim measures) (2001/165/EC) [2002] OJ L 59/18. At https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0165.

193 European Commission, 'Antitrust: Commission requires Daimler-Chrysler, GM, Fiat and Toyota to make car-repair information available to independent garages' (Press Release, 10 April 2007) at https://ec.europa.eu/commission/presscorner/detail/en/ip_07_1332. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

actual degree of use.

Similarly, a few years later, in 2011, the European Commission made legally binding the commitments offered by **International Business Machines Corporation (IBM)**[194]. In this case, the Commission feared that IBM was abusing its dominant position in the mainframe maintenance market by restricting independent service providers' access to essential spare parts. Mainframes are high-performance computers used by large companies and public institutions to handle critical business data. Commission market tested the commitments proposal and accepted them, under which IBM agreed to make spare parts and technical information promptly available to independent mainframe maintenance providers on commercially reasonable and non-discriminatory terms.

In the financial sector, two notable cases **of the European Commission** from 2011 and 2016 respectively, involved the imposition of data-access remedies[195]: the **investigation into the Credit Default Swaps (CDS) marke**t and the case concerning **Reuters Instrument Codes (RICs)**.

CDSs are traded either "over the counter" - where most transactions occur – or on exchanges. Trading platforms wishing to offer exchange-traded CDS products must access specific intellectual property, namely the CDS indices and the Final Price, which is used following the default of a debit obligation to determine payments between buyers and sellers of linked CDS contracts[196]. In its investigation, the European Commission expressed concerns that the International Swaps and Derivatives Association (ISDA) – a trade organization representing over 850 financial institutions – together with the

194 European Commission, 'Antitrust: Commission makes IBM's commitments legally binding to ensure competition in mainframe maintenance market' (Press Corner, 13 Dec 2011) at https://ec.europa.eu/commission/presscorner/detail/en/ip_11_1539.

195 The relevance of these cases was highlighted by the European Commission in its response to the Questionnaire.

196 European Commission, 'Antitrust: Commission accepts commitments by ISDA and Markit on credit default swaps' (Press Release, 20 July 2016) <https://ec.europa.eu/commission/presscorner/detail/en/ip_16_2586>. Accessed 30 March 2026.

financial information provider Markit and several investment banks, had refused to license the Final Price and the CDS indices (CDX and iTraxx) for exchange trading. The competitive concern therefore centered on the licensing of the intellectual property needed to offer CDS trading services.

The parties proposed commitments, which, after market testing, were accepted by the Commission. These commitments ensure that all trading platforms receive fair, reasonable and non-discriminatory (FRAND) access to the data and intellectual property held by ISDA and Markit. ISDA committed to license its rights over the Final Price on FRAND terms for exchange trading, and Markit agreed to license the iTraxx and CDX indices on FRAND terms for exchange-traded financial products based on its indices.

The second financial-sector case refers to the Commission's concern that Thomson Reuters might be abusing its dominant position in the market for consolidated real-time datafeeds through restrictive licensing practices[197]. To remedy these concerns, Thomson Reuters offered commitments, which, after two market tests and improvements, were accepted by the Commission. Under the commitments, Thomson Reuters was required to introduce a new license (the "ERL") allowing customers to use Reuters Instrument Codes (RICs) for data sourced from Thomson Reuters' competitors, for a monthly fee. These RIC codes are used to identify securities by financial institutions to retrieve data from Thomson's real-time datafeeds. The commitment enables customers to switch to competing providers of consolidated real-time datafeeds for both server-based and desktop-based applications covered by global licenses. The ERL is available for subscription for five years and can thereafter be converted into a perpetual license upon payment of a fee. Under the commitments, third

197 European Commission, 'Antitrust: Commission accepts commitments from Thomson Reuters in consolidated data-feeds market' (Press Release, 27 June 2012) <https://ec.europa.eu/commission/presscorner/detail/en/ip_12_1433>. Accessed 30 March 2026.

parties may also develop and maintain a switching tool that grants interoperability between RICs and competing services by translating RICs into other providers' financial identifiers.

A similar outcome emerged in the insurance sector through a decision by the **European Commission** in the **Insurance Ireland case**, which obliged an association of Irish insurers to grant access to a database they had developed, and which had become a *de facto* standard in the industry.

The European Commission found that the association restricted competition in the Irish motor insurance market by arbitrarily delaying or denying non-members access to its information-exchange system, *Insurance Link*, which was deemed essential for accurately assessing customer risk profiles. This conduct allegedly created entry barriers, particularly for insurers established in other Member States, ultimately limiting price competition and consumer choice. Following market testing, the Commission accepted commitments aimed to restore a level playing field and facilitate market entry[198] offered by Insurance Ireland, requiring the company to guarantee access to *Insurance Link* irrespective of membership status and to apply fair, objective, transparent, and non-discriminatory access criteria, applied uniformly to all companies, whether based in Ireland or in other Member States.

Finally, within the framework of the *ex-ante* **regulation implemented by the Digital Markets Act (DMA)**, it is worth noting the specification proceedings initiated by the **European Commission** in January 2026 (with decision still pending). Two proceedings were launched with the objective of guiding **Google**, as a gatekeeper, in complying with the obligations under the DMA. One of these proceedings concerns the obligation set forth in Article 6(11) of the DMA[199]. This provision

198 European Commission, 'Antitrust: Commission accepts commitments by Insurance Ireland to ensure access to its data sharing platform' (Press Release, 30 June 2022) at <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4242>. Accessed 30 March 2026.

199 The other proceeding concerns the obligation set forth in Article 6(7) of the DMA regarding the requirement to ensure free and effective interoperability between the Android opera-

requires Google to grant third parties providing online search engine services access to anonymized data held by Google Search – including rankings, queries, clicks, and views – under fair, reasonable, and non-discriminatory (FRAND) conditions. This type of proceeding is provided for under Article 8(2) of the DMA and enables the gatekeeper to obtain clarity regarding the specific measures it must adopt in order to ensure compliance. In this case, the Commission's measures act as data-related remedies, specifically related to data sharing, with the aim of allowing competing search engines to optimize their offerings and provide users with genuine alternatives to Google Search[200].

France

In 2017, the French competition authority **(Autorité de la concurrence – ADLC)** imposed a data-sharing remedy in consultation with the data protection authority (Commission Nationale de l'Informatique et des Libertés - CNIL) to former monopolist **GFD Suez** (Gaz de France Suez) with regard to its customers' consumption data offers an interesting example of a practical solution to this problem that may not be acceptable under modern data privacy legislation, such as the GDPR: the sharing was permitted based on the communication of the transfer to users and the offering of an opt-out, which arguably does not meet the threshold of a statement or by a clear affirmative action demanded by the legislation[201]. Data relating only to customers who have not formally objected to

ting system and third-party developers, particularly with respect to the functionalities used by Google's own artificial intelligence service, Gemini. The objective is to ensure that third-party AI service providers have access to the same technical functionalities as those available to Google.

200 European Commission, 'Digital Markets Act: Commission opens specification proceedings on Google's compliance', Press Release (26 Jan 2026) at <https://ec.europa.eu/commission/presscorner/detail/en/ip_26_202>. Accessed 30 March 2026.

201 GRAEF, I. THOMBAL, T., DE STREEL, A., 'Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law' Background Note for the meeting of the Digital Clearinghouse of 19 November 2019, available at <https://static1.squarespace.com/static/5cb4d40365a7070cc7d2d1fc/t/5ddf946ee6b0e7013a3622d7/1574933616451/DCH+-+Background+note+Final+website.pdf>. Accessed 30 March 2026.

the disclosure of their data will then be made available to the companies that requested it[202].

Italy

The **Italian competition authority** also indirectly addressed the issue of data access in a case concerning **Enel** and its conduct in the electricity markets[203]. According to the AGCM, the incumbent energy provider, Enel, vertically integrated in distribution and in the regulated market electricity supply, and which for many years had been the main beneficiary of the regulatory framework granting an exclusive right to provide the enhanced-protection service, had unfairly used the contact data of the regulated-market customer base, obtained through the privacy-consent mechanism, for commercial purposes in the liberalized market. The case indirectly touched upon data-access issues because no remedies of this nature were imposed; instead, the authority issued a cease-and-desist order and imposed an administrative fine.

Even though the case was later dismissed by the Supreme Administrative Court (*Consiglio di Stato*), in 2022 the European Court of Justice clarified in a preliminary reference proceeding that in markets undergoing liberalization – where specific information-sharing obligations exist within the limits established by data-protection rules – the resources available to the incumbent operator by virtue of its former legal monopoly must be equally accessible to its competitors[204].

202 Autorité de la concurrence, Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité (9 December 2014) at <https://www.autoritedelaconcurrence.fr/sites/default/files/commitments/14mc02.pdf, paragraphs 294-296>. Accessed 30 March 2026.

203 Autorità Garante della Concorrenza e del Mercato (AGCM), 'A511 - ENEL/CONDOTTE ANTICONCORRENZIALI NEL MERCATO DELLA VENDITA DI ENERGIA ELETTRICA Provvedimento n. 27494' at https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/2CA1849948BB53A4C1258383003A5D4E/$File/p27494.pdf. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

204 Case C-377/20, Judgment of the Court (Fifth Chamber) [2022] ECLI:EU:C:2022:355 at <https://curia.europa.eu/juris/document/document.jsf?text=&docid=259148&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12945319>, paragraphs 92 and 94. Accessed

Germany

One recent and interesting case on the data access remedy by the **German competition authority** is the **Deutsche Bahn (DB)** decision[205]. DB, a state-owned company, is vertically integrated from network operation to ticket distribution and is the incumbent rail operator in Germany.

The services of third-party mobility platforms need DB's travel data to offer their customers comparative information on itineraries involving different means of transport and transport operators as well as the option of integrated ticketing. Bundeskartellamt found that the company is not only a dominant rail operator, but it is also a strong mobility platform itself with its online portal bahn.de and its app DB Navigator. DB used its key position on the transport and infrastructure markets to restrict competition from third-party mobility platforms by denying third-party platforms continuous and non-discriminatory real-time access to essential traffic data, such as data on delays or train cancellations.

The Bundeskartellamt qualified these practices as infringements of Article 102 TFEU and Section 19 GWB. As a remedy, the authority imposed the duty to grant third-party mobility platforms real-time, non-discriminatory access to the relevant traffic data[206]. DB appealed the decision before the Düsseldorf Court of Appeals, but on 8 March 2024 the court largely rejected DB's interim measure request. In August 2024, Bundeskartellamt published that DB had implemented the measures by entering into first agreements with mobility

30 March 2026.

205 Bundeskartellamt, 'Open markets for digital mobility services – Deutsche Bahn must end restrictions of competition' (Press Release, 28 June 2023) at <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/28_06_2023_DB_Mobilitaet.html?nn=3591568>. Accessed 30 March 2026.

206 Silke Heinz, 'Main Developments in Competition Law and Policy 2023 – Germany' (Wolters Kluwer Competition Blog, 5 March 2024) at <https://legalblogs.wolterskluwer.com/competition-blog/main-developments-in-competition-law-and-policy-2023-germany/>. Accessed 30 March 2026.

platforms granting the real-time data[207].

United States of America

In the USA, a data-sharing decision was issued **by US District Court of Columbia (judge Mehta)** following a suit by the US Department of Justice and 11 states filed a complaint accusing **Google** of unlawful monopolization of the online search and search advertising markets[208].

Plaintiffs argued that Google entered into contracts with browser developers, mobile device manufacturers, and wireless carriers to pre-install Google Search as the default general search engine and other agreements that amounted to exclusivity of Chrome, Google Assistant, and the Gemini app. In August 2024, the court held that Google unlawfully maintained a monopoly in general search and search advertising, primarily through agreements that foreclosed rivals' access to users and scale because they strongly disincentivized Google's distribution partners from preinstalling rival search engines. The court found that these contractual practices reinforced a feedback loop in which Google accumulated disproportionate volumes of search queries and click-and-training data, thereby strengthening its algorithms and further entrenching its dominance.

In response to the competitive harms, in September 2025, the remedies sought in the case focused on prohibiting exclusivity agreements related to the distribution of Google Search, Chrome, Google Assistant, and the Gemini app. In addition to those remedies clearly linked to the conduct at stake, plaintiffs claimed that a more comprehensive set of

207 Bundeskartellamt, 'Further important step in implementing the Bundeskartellamt's ruling on abusive practices against Deutsche Bahn – mobility platforms gain access to real-time data' (Press Release, 15 August 2024) at <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2024/15_08_2024_Deutsche_Bahn.html?nn=55030>. Accessed 30 March 2026.

208 *United States et al. v. Google LLC* (2020). See <https://www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc>. Accessed 30 March 2026.

remedies was needed, including in relation to data sharing. The reason for this broader scope was the need to restore competition which is made more difficult here as a reflection of the relevance of network effect that Google has enjoyed. The Court accepted this claim and noted that the volume and breadth of data-sharing ordered would not work as a *de facto* divestiture of Google's intellectual property and therefore needed not be treated as a structural remedy that must be supported by "a clearer indication of a *significant causal connection* between the conduct and creation or maintenance of the market power." In essence, the mandated sharing of the fruits of the violation must not be "attributable entirely" or in "predominant part" to the unlawful act: such a high standard would allow a monopolist to continue benefitting from its violation simply by merely pointing to *some* lawful factors for its success, and it would hamstring trial courts in the exercise of their equitable authority to restore competition.

Per the plaintiffs' request, Google would need to provide certain qualified rivals with access to search-index data, ad data and user-interaction information.

The *search index* is the database of publicly accessible webpages retrievable in response to user queries. Plaintiff requested, in particular, that Google makes available, "at marginal cost," the following information: (1) the unique identifier (DocID) for each document in the search index and a notation sufficient to denote duplicates of such documents; (2) a DocID to URL map (i.e., data that corresponds the unique DocID to a page's address on the web); and (3) for each DocID "a set of signals, attributes, or metadata associated with each DocID that are derived in any part from User-side Data,including but not limited to (A) popularity as measured by user intent and feedback systems including Navboost/Glue, (B) quality measures including authoritativeness, (C) time that the URL was first seen, (D) time that the URL was last crawled, (E) spam score, (F) device-type flag, and (G) any other specified

signal the [Technical Committee] recommends to be treated as significant to the ranking of search results."

However, the Court narrowed down this request, by removing open-ended formulations that may end up forcing the disclosure of data that has only remote connection with the harm, like "any signal, attribute, or metadata derived in any part from User-side Data" or the ability of the Technical Committee to include any signal "significant to the ranking of search results." On grounds of proportionality, the court declined to mandate sharing of two of the user-side datasets specified by Plaintiffs that rely in part on user-interaction data ("popularity as measured by user intent and feedback systems including Navboost/Glue" and "quality measures including authoritativeness" associated with each DocID") as well as a third dataset (the "knowledge graph) that is composed of information given by local businesses and interested third parties, rather than as a result of users' navigation on Google.

It also refused to order the sharing of such data on a "periodic basis to be determined by the Plaintiffs in consultation with the [Technical Committee]", allowing rivals to receive only a one-time snapshot of the relevant data. This was deemed in line with the goal of this part of the remedy, which was to give competitors a one-time ladder to make up for the scale gap, not a continuous subsidy over time. Importantly, the remedy was concerned with the ability to build a better machine for search results, and not with its monetization through advertising. For this reason, the court declined to order the disclosure of data that did not come directly from user interaction with Google, which it viewed as the primary fruit of Google's distribution agreements.

As for the *user-interaction data*, this concerns links users select and the amount of time they pause over them. The court characterized this "click-and-query" information as the fundamental input Google relies on to refine its search services

and as a key component of the scale advantage it enjoys. Per the Plaintiffs'request, this data includes (1) User-side Data used to build, create, or operate the GLUE statistical model(s); (2) User-side Data used to train, build, or operate the RankEmbed model(s); and (3) The User-side Data used as training data for GenAI Models used in Search or any GenAI Product that can be used to access Search.

Once again, however, the court narrowed down the request to carve out n. (3), due to the lack of sufficient evidence over what type of data is used, and to what extent, in the training of GenAI, and therefore of the significance of Google's scale advantage in the context of GenAI search-assisted response.

It is interesting to note that here the Court saw the need for a more than one-time disclosure, given the importance of updating training data with fresh information. Nevertheless, it decided to set a cap on the number of such disclosures that can occur during the term of the judgment, with the specific limit to be determined in consultation with the Technical Committee. In the words of the court, a cap protects against Qualified Competitors free riding on Google's data, and it will lessen the burdens associated with implementing privacy measures that will have to be applied before disclosure occurs.

All in all, the remedy reflects an understanding that in search markets, data may not be merely an output of market success, but a reinforcing input that can perpetuate monopoly power. As such, the remedial framework attempted to restore contestability not only by removing contractual restraints, but also by rebalancing access to the data necessary for effective competition.

Japan

Returning to **Google/Fitbit**, but now looking at the **JFTC's decision**, in addition to the data-segregation remedies

proposed by the parties, Google also committed to maintain the access of certain health-related data (specifically, supported measured body data) to health-related application providers outside the Google Group, via the Web API offered by the parties, free of charge, for a period of ten years from the date of the acquisition. This commitment is conditional upon the consent of general consumer users and must be implemented in accordance with the terms and conditions governing the use of the Fitbit platform[209].

Another merger decision taken by the **JFTC** in which a data-access remedy was applied was the review of the **acquisition of shares of Nihon Ultmarc Inc.**, a company with a substantial market share in the medical information database provision business, **by M3, Inc.**[210], which operates and manages pharmaceutical information platforms that provide doctors with advertising and information on the proper use of prescription drugs and related topics.

Although the acquisition did not meet the notification thresholds set out in the Antimonopoly Act, it raised competitive concerns and the JFTC therefore reviewed the transaction. The JFTC approved the acquisition subject to remedies proposed by the parties. In light of the competition concerns relating to input foreclosure, the parties were required to not refuse providing their competitors (including new entrants) in the pharmaceutical information platform market with access to their Medical Databases and other relevant databases, for an indefinite period following the implementation of the acquisition. Furthermore, the merger parties were required not to engage in discriminatory treatment of any competitors with respect to pricing, as well as the content, quality, and

209 Japan Fair Trade Commission (JFTC), 'The JFTC's Review Results concerning Acquisition of Fitbit, Inc. by Google LLC (January 2021) at <https://www.jftc.go.jp/en/pressreleases/yearly-2021/January/210114r.pdf>, p. 26. Accessed 30 March 2026.

210 Japan Fair Trade Commission (JFTC), Press Release. 'The JFTC Reviewed the Acquisition of Shares of Nihon Ultmarc Inc. by M3, Inc.' (24 October 2019) at https://www.jftc.go.jp/en/pressreleases/yearly-2019/October/191024.html. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

other commercial terms governing the provision of Medical Databases, also for an indefinite period from the date of the acquisition[211].

(v) Data control enhancement

Definition

Data control is a principle which implies an ability for data subjects to decide over the terms of processing their own personal data, which can only be achieved through an effective oversight on data processing operation[212]. It can be exercised both in individual and in a collective form, and can be enhanced through design features, governance arrangements or other accountability mechanisms.

To some scholars, the stringency of the conditions imposed by the GDPR and similar frameworks for valid reliance on consent reflects unease with the range of issues affecting privacy "self-management" as a valid model of protection[213]. For Solove, the inadequacy of that model is due both to cognitive as well as structural issues affecting the ability of data subjects to adequately assess costs and benefits associated with consenting to certain processing: "because individual decisions to consent to data collection, use, or disclosure might not collectively yield the most desirable social outcome, privacy self-management often fails to address these larger social values"[214]. For this reason, alternative solutions usually involve collective mechanisms for oversight and control, such as data trusts and cooperatives.

211 Japan Fair Trade Commission (JFTC), 'Results of review on the acquisition by M3, Inc. of the shares in Nihon Ultmarc Inc.' (October 2019) at <https://www.jftc.go.jp/en/pressreleases/yearly-2019/October/191024r.pdf>, p. 15. Accessed 30 March 2026.

212 See, for instance, Graef, I., Husovec, M. and Purtova, Nadezhda. TILEC Discussion Paper 'Data portability and data control: lessons for an emerging concept in EU law" (2017), p. 2 and 5."[...] the regulation of the allocation and extent of control over data, i.e. by way of exclusive rights or possibilities of access, becomes increasingly important. Put differently, the shape and direction of data flows, as well as varieties of data-enabled business models and the ways of drawing value from data will largely depend on who gets access to data, under what circumstances, for what purpose or who is precluded from access, can move or keep their data assets to itself or is obliged to share data with others" and "According to Recital 68 of the final version of the GDPR, the RtDP shall 'further strengthen [data subjects'] control' over their personal data".

213 Daniel Solove, "Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126 (2013): 1880.

214 Solove, *Id.*, 1881.

"Trust" is a legal characterization that encompasses a range of related concepts[215]. In general terms, it is a form of property holding where the receiver (trustee) must apply the property exclusively for the benefit of someone else (beneficiary), whose identity may or may not coincide with that of the person who set up the trust (settlor).

Other than by natural and legal persons, trusts may be the result of judicial or legislative creation. In all these cases however, independently from their origin, trustees have two different duties towards their beneficiary: first, a fiduciary duty of undivided loyalty, which implies that the trustee must act in the sole interest of the beneficiary (and therefore cannot assume any conflicting interest); second, a duty of care, which implies that they should exercise reasonable care in the handling of the property. Recent work has applied these characteristics to arrangements whereby one or more individuals are entrusted with the holding of data, arguing that this instrument is flexible enough to permit the emergence of a variety of trusts, each of which would negotiate with data collectors on the beneficiary's behalf in accordance with the rules and values enshrined in each particular governing statute[216].

In some cases, data trustees can also be public entities that are assigned with the responsibility to manage datasets (in particular in the health sector) in accordance with predefined criteria, often including granting vetted access to third parties, and therefore play a role that is also known in some jurisdictions as one of "data custodian"[217].

---

215 Charlie Webb & Tim Akkouh, *Trusts Law* (Fifth ed., Palgrave 2017), p. 1.

216 Sylvie Delacroix, Neil D Lawrence, Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance, International Data Privacy Law, Volume 9, Issue 4, November 2019, Pages 236–252.

217 See, for instance, Western Australia´s Data Stewardship and Custodianship Policy (2016), available at <https://ww2.health.wa.gov.au/~/media/Files/Corporate/Policy%20Frameworks/Information%20management/Policy/Data%20Stewardship%20and%20Custodianship%20Policy/Data-Stewardship-and-Custodianship-Policy.pdf> accessed 1 December 2020. The definition for data custodian refers to: " The person(s) responsible for the day-to-day management of a data collection, as nominated by the Data Steward. Data Custodians assist the Data Steward to protect the privacy, security and confidentiality of information within data collections. Data Custodians also aim to improve the accuracy, usability and accessibility of data within the data collection". In turn, the definition provided for "Data Steward" is :" A position with delegated responsibility from the Director General of the Department to manage a data collection. The Data Steward's primary responsibility is to protect the privacy, security and confidentiality of information within data collections. Data Stewards also approve the conditions for appropriate use and disclosure of information for clearly defined purposes that comply with WA Health's statutory obligations and Information Management Policy Framework."

Regardless of the formal qualification, the important feature from the standpoint of competitive analysis is that they lead to trustees managing the interests of various groups of society. This can have positive effects in allowing their beneficiaries to overcome a weak bargaining position and be heard more effectively within society, but also the negative effect of potentially extending the effects of market power held by any of the represented stakeholder groups. Both individual and collective control solutions can be imposed through competition remedies, presenting challenges on the development of effective control rights. However, collective solutions raise additional challenges in terms of preventing possible side-effects from the newly created mechanisms of coordination, which need to be parsed out in connection with the levels of integration and collaboration[218].

Finally, one should bear in mind that enhancement of data control need not refer to data subjects or end users, it could also be a remedy targeted at business users. As long as a remedy obliges one or more undertakings to provide more options to another stakeholder in relation to the processing of data that concerns them, it will fall within the scope of this typology. Important also to note that these options need to go beyond mere transparency or the ability to download and/or transfer data, as that is already covered by data transparency and portability (which fall into other categories, as previously discussed).

Application

Germany

In the context of unilateral conduct, a notorious remedy involving enhanced control over personal data is the **German competition authority** (**Bundeskartellamt)**´s decision in the **Facebook** case, which was found to have abused its dominant position by imposing unfair terms and conditions to its users that involved the collection of data from third party sites without

218 Zingales, N. (2022). "Chapter 1: Data collaboratives, competition law and the governance of EU data spaces". In *Research Handbook on the Law and Economics of Competition Enforcement*. Cheltenham, UK: Edward Elgar Publishing.

adequate consent[219]. Following this finding, the authority ordered Facebook to come up with a technical solution which ensures that transfers of such data onto Facebook is stopped, with the exception of those based on a free and informed consent of each concerned user.

Although some suggest this order could have been implemented by simply prohibiting the transfer of third-party data to Facebook, a less restrictive option was chosen by Facebook: ensuring appropriate consent for the transferring of such data onto Facebook. After lengthy discussions, the authority validated the solution chosen by Facebook through a modified central accounting system making the overall user journey significantly more transparent and comprehensible[220]. However, the Bundeskartellamt also alerted that it remains to be clarified how users can be informed as correctly and neutrally as possible about the use and data processing consequences involved in Meta's Business Tools and plugins (e.g. Facebook Login, "Like" button) in a central location and how they can consent to or reject the use of their data in a simple way, and under which exceptional circumstances data processing across accounts can be legal even without the users' consent (e.g. for security purposes)[221].

It should be noted that, given the similarity of issues raised by competition and data protection law in this case, the Bundeskartellamt regularly exchanged views with (and received no objection from) the German data protection authorities during the proceedings. In addition, the Bundeskartellamt was supported on technical issues by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). The Federation of German Consumer Organisations (Verbraucherzentrale

219 BundesKartellAmt. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_2023_Meta_Daten.html?nn=295782

220 See more at: <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_2023_Meta_Daten.html?nn=295782>. Accessed on October 30, 2025.

221 Id.

Bundesverband, vzbv) was also involved in the proceedings as a third party[222].

In 2021, based on the new amendment to the GWB, the **Bundeskartellamt** opened proceedings against **Google** (Case B7-70/21), which focused on the collection and processing of data and the choices provided to users – as described in Section 19a(2) sentence 1 no. 4a GWB. In December 2022, the Bundeskartellamt then presented Google with a preliminary assessment notice indicating that Google would be prohibited from using and implementing data processing terms that do not offer its end users sufficient choice (granular, free, and informed) to consent or not to that processing of their data[223].

In light of this preliminary assessment, Google and the authority engaged in dialogue to reach a consensual solution, and Google submitted a proposal for commitments, which the Bundeskartellamt made binding in its October 2023 decision[224]. The main objective of Google's commitments is to provide users with transparent choices, allowing them to make informed decisions about how their personal data is used across services, especially when personal data from a Google service is combined with data from other sources (whether from Google or not) or when data is used in Google services offered separately[225]. Thus, Google has committed not to process any user data between its own services or between Google and third-party services without valid user consent – which can only be requested based on a free and informed

222 Id.

223 Bundeskartellamt, OECD. 'The intersection between competition and data privacy – Note by Germany' (13 June 2024) at <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2024/OECD_2024_intersection_between_competiton.pdf?__blob=publicationFile&v=3>. Accessed 30 March 2026.

224 Bundeskartellamt, '*Decision pursuant to Section 19a(2) sentence 4 in conjunction with Section 32b(1) GWB*', 7th Decision Division – Case B7-70/21 (5 October 2023) at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf?__blob=publicationFile&v=2>. Accessed 30 March 2026.

225 Bundeskartellamt, 'Bundeskartellamt gives users of Google services better control over their data' (Press Release, 05 October 2023) at <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/05_10_2023_Google_Data.html>. Accessed 30 March 2026.

choice by users. In short, Google cannot set consent as the default option for its users.

A third case by the **Bundeskartellamt** that should be mentioned is **Apple ATT**, where the authority is currently market testing the commitments proposed by Apple in response to competition concerns related to its App Tracking Transparency Framework (ATT)[226]. Since the framework's implementation in 2021, third-party app developers distributing applications through the iOS App Store have been required to obtain explicit user consent before accessing certain data for advertising purposes.

The authority's preliminary assessment found that these strict consent requirements applied exclusively to third-party providers, while Apple itself was not subject to equivalent constraints. Differences in the design and presentation of consent prompts appeared to favor Apple's own services, as they were more likely to encourage user consent, whereas third-party prompts were less user-friendly[227]. In response, Apple's proposed commitments include revisions to the two principal consent interfaces: the ATT prompt used for third-party applications and the prompt governing Apple's own data collection practices.

In sum, Apple has committed to redesigning both prompts to ensure neutrality align the wording, content, and visual presentation of consent requests, in order to provide clearer and more accurate explanations for its users of the technical processes involved following their consent. These modifications may ensure that users can make informed decisions under conditions that do not unduly favor Apple's services over its competitors. However, Apple has not proposed changes to its advertising attribution practices, which currently allow the

226 See <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2025/12_02_2025_ATTF.html>. Accessed 30 March 2026.

227 See <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2025/02_13_2025_ATTF.html?nn=48888>. Accessed 30 March 2026.

company to measure advertising success without obtaining prior user consent. The competition authority has expressed reservations regarding this approach and will evaluate, through the ongoing market test, whether it continues to place third-party providers at a competitive disadvantage. If accepted, Apple's commitments will operate as competition remedies that aim to enhance user autonomy and transparency in relation to how their data are used, while ensuring that consent mechanisms comply with competition law principles and do not distort competitive conditions in digital markets.

A parallel case on **Apple's ATT program** has been decided by the **competition authorities in France (Autorité de Concurrence) and Italy (AGCM)**, and is under examination by the **Brazilian competition authority (CADE)**.

France

In **France**, the **Autorité** found that the **ATT framework imposed by Apple** is not necessary, insofar as the consent obtained is not valid under the applicable laws, in particular the French Data Protection Act. It noted that the rules governing the interaction between the different pop-up windows displayed undermine the neutrality of the framework. However, despite imposing a fine of €150,000,000, the Autorité fell short of imposing any remedy.

It is worth noting that the Autorité received two opinions from the CNIL on various questions relating to the applicability of privacy legislation raised by the case, which the Autorité took into account in its competitive analysis (one in support of the decision over the issuance of interim measures, and the other before ruling on the merit)[228]. These two opinions showed that bringing the ATT pop-up into compliance with competition law would not have led Apple to downgrading

228 See <https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising--autorite-de-la-concurrence-imposes-fine-eu150000000-apple>. Accessed 30 March 2026.

the effectiveness of its privacy protection system. Invited by the Autorité to comment as part of the investigation into the merits, the CNIL stated that: "making publishers systematically collect user consent twice for the same purpose constitutes an unnecessary and artificial complexity".

Italy

In Italy, the AGCM fined Apple € 98.635 for violation of article 102 TFEU, due to the imposition on third-party developers of non-objective, non-transparent and non-proportionate conditions which could guarantee an economic benefit to Apple itself[229]. Like the Autorité, AGCM did not impose any remedy, and conducted consultations with the data protection authority (Garante). What is worth highlighting, however, are the details about the extent of the interactions between these authorities, as well as the specific reference by AGCM of the opinion of the data protection authorities in other jurisdictions (Germany and France).

First, on 2 April 2024 AGCM submitted a specific request to Garante, responded on 7 May 2024 by explaining responsibilities under data protection law, whilst expressing concerns about the way in which Apple's framing of consent request prevented an effective understanding and hindered the autonomy of developers in choosing the means and purposes of processing of personal data. Second, on 23 June 2025, AGCM consulted the Garante once more, receiving in response a confirmation that the solutions implemented by Apple are a result of the company's own commercial choices, rather than an inevitable application of the law. Garante also clarified specifically that the law does not impose the need for a double consent, as alleged by Apple. It should be mentioned that Garante specified in its first interaction with AGCM that

229 See <https://en.agcm.it/en/media/press-releases/2025/12/A561?__cf_chl_tk=4i3Mxo-0ajQ7qOQPjfPn_aKXtzjID.m82Anc88n7JIDU-1772332240-1.0.1.1-o336PLy9ZdqGgsJqFrlXK_iIp-Jvbp3T4hRetZuGseBQ>. Accessed 30 March 2026.

it examined the case "maintaining a particular interest for any initiative that permit to increase the safeguards beyond the minimum level", and recognizing the existence of "several considerations that do not fall within the sphere of competence of Garante"[230].

(vi) Application of Privacy Enhancing Technologies

In theory, Privacy Enhancing Technologies can be used to reduce the risks of (re)identification and the adverse effects of data processing, thereby improving the feasibility of data remedies.

In the **US District Court for the DC Circuit decision** against **Google**[231]Judge Metah required Google to use privacy-enhancing techniques such as adding noise, generalization, suppression, query-intent grouping and k-anonymity to minimize the risk to privacy associated with the shared datasets. It did not prescribe any particular solution, however, and left this assessment to the Technical Committee that oversees the implementation of the remedy, being required to (i) recommend reasonable data security standards applicable to Qualified Competitors; and (ii) consult with Plaintiffs about appropriate User-side Data security and privacy safeguards. Indeed, the court envisaged that the "all- important application of privacy-enhancing techniques to anonymize User-side Data" represents one of the key challenges in the implementation of the remedy package.

(vii) Data Transparency

Definition

Where transparency is a requirement for effective oversight on a firm's conduct, the imposition of specific disclosure rules may constitute an appropriate remedy. One should distinguish, however, transparency

230 Decision, para. 409.

231 See <https://storage.courtlistener.com/recap/gov.uscourts.dcd.223205/gov.uscourts.dcd.223205.1436.0_1.pdf>. Accessed 30 March 2026.

vis a vis the customers of a firm and transparency *vis a vis* a regulatory authority. The latter is frequent in regulated industries in order to facilitate monitoring over potentially problematic conduct, including possible ways of evading the applicable regulatory requirements[232], and naturally lends itself to cooperation between the antitrust enforcer and the regulator in the design and enforcement stage. The former is less common but mostly occurs when a dominant company puts its business partners at disadvantage by not defining sufficiently clear rules of engagement and thus retaining the discretion to apply them inconsistently (and potentially, discriminatorily). The former type of transparency remedy has also significant implications for collusive conduct, often leading to price increases by creating focal points[233]. Both typologies, however, are united by a defining feature: they are necessary to pierce the veil of opacity that characterizes certain aspects of a firm's operation and obtain more effective oversight on its conduct.

Terms of service and privacy policies of online websites are said to be a natural first port of inquiry to assess the legitimacy of personal data processing under data protection law. They constitute an important means by which data controllers implement their duty under the GDPR to provide data subjects with the required information over collection and use of personal data: the legal basis and purposes of the processing[234], the categories of the data concerned[235], the policy concerning their storage period[236], the recipients or the categories of recipients[237], the existence of transfers to third countries or international organizations[238], and any legitimate interest of the controller or a third party which is relied upon to justify processing[239]. They would also typically contain

232 US DEPARTMENT OF JUSTICE, Merger Remedies Manual (2020). <https://www.justice.gov/atr/page/file/1312691/dl?inline=>. Accessed 30 March 2026.

233 CADE, Guide to Antitrust Remedies (2018), at <https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/Guide-Antitrust-Remedies.pdf>. Accessed 30 March 2026.

234 Art. 13 (c) and 14 (c).

235 Art. 14 (1) (d).

236 Art. 13 (2) (a) and 14 (2) (b).

237 Art. 13 (1) (e) and 14 (1) (e).

238 Art. 13 (1) (f) and 14 (1) (f).

239 Art. 13 (1) (d) and 14 (1) (b).

information about the existence, significance and consequences of solely automated decision-making which produces legal or otherwise significant effect on a data subject[240], forming the basis for any explicit consent or contract with the data subject upon which such decisions could be justified[241]. The rationale of these information duties is to enable individuals to appreciate the risks, rules, safeguards and rights involved in the processing[242], with a view to exercising informed choices in their relationships with data controllers.

To facilitate that process, the GDPR introduces the requirement to provide such information in a concise, transparent, intelligible and easily accessible form, and using a clear and plain language – especially when directed to a child[243]. In its 2017 Guidance on Transparency, the Article 29 Working Party ("A29WP") suggested that "Concise and transparent" requires an efficient and succinct presentation, so as to avoid information fatigue[244]; it also evoked in that sense the idea of a layered privacy notice, which links to the Regulation's more general reference to "appropriate visualization" techniques[245]. It also presents a definition of the "clear and plain language" component: according to the A29WP, this means that, in particular in relation to the purposes and legal basis for processing, "the information provided should be concrete and definitive [...] not phrased in abstract or ambivalent terms or leave room for different interpretations".[246] This interpretation rules out the admissibility of broad formulations of purpose such as: "We may use your personal data to develop new services", "We may use your personal data for research purposes" and "We may use your personal data to offer personalized services".

240 Art. 13 (2) (f) and 14 (2) (g).

241 Art. 22 (2).

242 Recital 39.

243 Art. 12 (1).

244 Para. 7.

245 Recital 58.

246 Para. 11.

Data protection legislation in other jurisdictions is consistent with this approach, even when offering a less detailed guidance[247]. These benchmarks may be used to raise the level of transparency *vis a vis* data subjects.

Other data transparency interventions involve the explanation of criteria and the decision-making process used for ranking, suspension and removal of content or accounts, as is done through the EU Platform to Business Regulation[248] with regard to online intermediation services. Note that the Regulation is concerned especially with transparency *vis a vis* business users or corporate website users and therefore is complementary to the protections already existing in data protection or consumer protection legislation.

Finally, data transparency requirements have been introduced for gatekeepers providing advertising services in order to enable scrutiny of their practices. Namely, Articles 5(9) and 5(10) of the DMA require gatekeepers to disclose to publishers and advertisers sufficient information to make sense of the prices they are billed for the gatekeeper's online advertising services, enhancing transparency and strengthening these actors' ability to monitor and steer their own dealings and spend. Article 6(8) complements this by obliging gatekeepers to provide information that lets the same parties independently check ad inventory and use the gatekeeper's performance-measurement tools. These may all serve as references for the implementation of data transparency remedies.

247 The ICN Handbook recognizes that certain "privacy guard rails" may ensure competition in markets. Among these regulatory "guard rails", particular emphasis may be placed on the regulations limiting or requiring individuals to opt out of behavioral advertising and personalized recommendations. For instance, California Privacy Rights Act, §2(l), states that consumers have right to opt out of having sensitive personal information used for behavioral advertising or shared to third parties for behavioral advertising. The ICN Handbook also refers to the 2018 Facebook case, in which the Italian authority (AGCM) found that there had been exploitation of users' personal data in the context of the zero-price/data-driven economy**.** Furthermore, in 2021, the AGCM also fined Google for abusive practices related to the omission of information regarding the collection and use of personal data, as well as the set-up of an opt-in as default option for data sharing consent. Cf. ICN, 'Competition law enforcement at the intersection between competition and privacy: agency considerations', 2024, p. 4 and 14.

248 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance). PE/56/2019/REV/1. OJ L 186, 11.7.2019, pp. 57–79.

Application

France

An illustration of transparency remedies towards business partners is the **Autorité**'s decision on **Google´**s suspension of the Adword account of **Navx**, a company selling digital-only databases for GPS navigation devices indicating the localization of fixed and mobile speed cameras[249]. Google motivated the suspension on ground of changes to its (previously more permissive) content policy for devices aimed at evading road traffic speed cameras in France, but the French competition authority established in a non-objective, non-transparent and discriminatory way which harmed some suppliers of radar databases.

As a result, while preserving Google´s freedom to create its own policy, the authority required the company to implement it in a transparent and objective fashion, not resulting in a discriminatory treatment. Google then offered the following commitments with regard to devices aimed at evading road traffic speed cameras in France:

> (i) making a clearer distinction between those navigation devices for which advertising is authorized and those which are prohibited, notably for warning devices and radar databases;
>
> (ii) defining better the scope of the prohibition, in particular whether it applies to the adverts' content only or if it also applies to the advertiser's destination pages or cross-referenced pages as well as to the use of keywords;
>
> (iii) introducing a procedure of information and notification targeted to the companies concerned regarding the modifications made to AdWords content

249 Autorité de la Concurrence, Décision n° 10-D-30 du 28 octobre 2010 relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet. <https://www.autoritede-laconcurrence.fr/sites/default/files/commitments//10d30.pdf>. Accessed 30 March 2026.

policy, (e.g. more restrictive changes have to be announced with three month notice, except for specific cases); and

(iv) making more precise the procedure that may lead to the suspension of the account of an advertiser in case of breach of AdWords content policy, which would involve at least two stages and a formal warning making the advertiser aware of the breach and of the risk of the suspension of its account.

A second case involving **Google** concerns essentially an identical conduct, but is more consequential due to its scope: the decision by the **Autorité** relates to the rules for advertisers to operate on **Google Ads**, and the remedy was part of an infringement decision imposing a fine, not the object of a voluntary commitment[250]. The final order required Google to

(i) clarify the drafting of the Rules of its Google Ads advertising platform and review the information procedures concerning changes to the Rules (individual notification two months before the change of Rule);

(ii) clarify the procedures for suspending accounts in order to prevent them from being brutal and unjustified;

(iii) put in place procedures for alerting, preventing, detecting and dealing with breaches of its Rules, so that the measures for suspending sites or Google Ads accounts are strictly necessary and proportionate to the objective of consumer protection;

(iv) organize mandatory annual training for staff responsible for providing personalized support to companies present on Google Ads so that the teams are sufficiently informed of the content and scope of the Google Ads Rules, as well as the risks that their customers

250 Décision n°19-D-26 du 19 décembre 2019 relative à des pratiques mises en œuvre dans le secteur de la publicité en ligne liée aux recherches. <https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-02/19d26.pdf>. Accessed 30 March 2026.

and users incur if they do not comply; and

(v) provide the Authority with an annual report specifying in particular the number of complaints filed against it by French Internet users, the number of sites and accounts suspended, the nature of the Rules violated and the terms of the suspension.

Germany

In Germany, enhanced transparency was part of a remedy package adopted voluntarily by **Amazon** in response to the **Bundeskartellamt**´s investigation on the use of abusive terms of business and related practices, including provisions limiting liability to the disadvantage of sellers, the choice of law and jurisdiction clauses, the rules on product reviews, the non-transparent termination and blocking of sellers' accounts, the withholding or delaying payment, and clauses assigning rights to use the information material which a seller has to provide with regard to the products offered and terms of business on pan-European dispatch.

On 17 July 2019, the Bundeskartellamt closed the investigation accepting the commitment offered by Amazon on a global scale (thus assuaging simultaneously similar concerns raised by the Austrian competition authority, who thereby closed the investigation) and including, among other provisions, that: (i) termination and suspension of sellers' accounts will only be possible upon provision of statement of reasons and following a 30 day notice period; and (ii) more salience and traceability for the rules and regulations applicable to sellers, and right to receive 15 days' notice for any changes thereto[251].

251 HEINZ, S., ´Bundeskartellamt ends abuse probe after Amazon agrees to changing business terms for dealers´, Kluwer Competition Blog (30 July 2019) at <http://competitionlawblog.kluwercompetitionlaw.com/2019/07/30/bundeskartellamt-ends-abuse-probe-after-amazon-agrees-to-changing-business-terms-for-dealers/>. Accessed 30 March 2026.

European Union

In 2020, the **European Commission** opened an investigation to assess whether the criteria used to select the Buy Box winner and to admit sellers to the Prime programme resulted in favourable treatment for Amazon's own retail business or for sellers using its logistics and delivery services (Case AT.40703 – Amazon Buy Box).

The Commission preliminarily found that these rules create unduly advantages both Amazon and sellers relying on its fulfilment network. To address these concerns, Amazon proposed to commit to

> (i) treating all sellers equally when ranking offers for the Buy Box and displaying a second competing offer to the Buy Box winner if there is a second offer from a different seller that is sufficiently differentiated from the first one on price and/or delivery; and
>
> (ii) applying non-discriminatory conditions for Prime eligibility, allowing Prime sellers to freely choose any carrier for their logistics and delivery services, and refraining from using any data on the terms or performance of third-party carrier obtained through Prime to benefit its own logistics services[252].

After the market test, Amazon strengthened its proposal by enhancing transparency and providing earlier information to sellers and carriers about the commitments and their newly acquired rights, thereby facilitating sellers' switching to independent carriers. The investigation and the Commission decision also addressed Amazon's use of confidential data from independent retailers selling on its platform, a concern for which the remedies adopted were closer to a data use prohibition, as will be discussed later.

252 European Commission, 'Antitrust: Commission refers Amazon to the European Commission's competition enforcer' (Press Corner, 30 Nov 2022) at <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777>. Accessed 30 March 2026.

United States of America

In the **United States v. National Association of Realtors case** (2020)[253],the US DOJ investigated and challenged rules adopted by the National Association of Realtors (NAR) affecting competition in the market for residential real estate brokerage services, particularly those tied to the operation of Multiple Listing Services (MLSs), the central databases through which real estate listings and brokerage information are disseminated. In this case, the **DC Circuit District Court** accepted DOJ's proposed data-transparency remedy: NAR was required that MLS systems make visible to brokers and consumers the database with commissions offered to buyer agents. In particular, NAR could not enter into any behavior that 'prohibits, discourages, or recommends against an MLS or MLS Participant publishing or displaying to consumers any MLS database field specifying the compensation offered to other MLS Participants'. This obligation guaranteed that compensation data (previously obscured from consumers) would be viewable and comparable across listings. The measure addressed concerns that hidden commission terms prevented price competition, facilitated steering toward listings with higher commissions, and contributed to inflated transaction costs. By increasing transparency over compensation fields embedded within MLS data, the remedy sought to reduce information asymmetry, enable consumers to evaluate lower-cost brokerage options, and weaken the structural incentives that reinforced traditional commission levels.

Croatia

In the decision by the **Croatian competition authority** on **Grand Automotive LLP** already discussed above, data-transparency remedies were also imposed. First, **Grand**

253 See <https://www.justice.gov/atr/case/us-v-national-association-realtors-0>. Accessed 30 March 2026.

Automotive LLP committed to enhancing transparency and access to the technical information of the vehicle brands it distributes, by publishing on its website instructions in Croatian enabling independent repairers to access the online databases of Hyundai and Ford (and, following the acquisition of Renault Nissan Hrvatska d.o.o., those of Renault, Nissan and Dacia). The company was also required to maintain a customer-support service, available to third parties during business hours, to assist them in accessing these databases. In addition, it committed to requesting that the respective manufacturers of Ford and Hyundai vehicles make such information accessible in the local language and, until this is implemented, continue to provide the required customer support. With respect to Ford vehicles, given that the website "www.ford.hr" is owned by the manufacturer itself, Grand Automotive LLP was required to seek to have the relevant information included there; if that was not possible, it would publish the information on its own website. Finally, Grand Automotive LLP should include in the manuals of Hyundai vehicles - and, following the acquisition, in those of Renault, Nissan and Dacia - a clear notice stating that out-of-warranty repairs did not need to be carried out by authorized service centers for the warranty to remain valid[254].

Italy

A case decided by the **Italian competition authority** involving **Meta**[255] and concerning the musical works available on Facebook and Instagram, also illustrates the application of data transparency remedies.

254 Croatian Competition Authority, 'Case No UP/I 034-03/2022-02/005, URBROJ 580-11/107-2022-052', Conditionally Approved Concentration (Zagreb, 9 August 2022) at <https://www.aztn.hr/ea/wp-content/uploads//2023/03/UPI-034-032022-02005.pdf>. Accessed 30 March 2026.

255 Autorità Garante della Concorrenza e del Mercato (AGCM), 'A559 – META/SIAE, Provvedimento n. 31537' (Bollettino 18/25, 12 May 2025) at <https://www.agcm.it/dotcmsdoc/bollettini/2025/18-25.pdf>. Accessed 30 March 2026.

According to SIAE (the Italian Society of Authors and Publishers) – a copyright collecting society – negotiations with Meta had been ongoing since 2022, but were interrupted in 2023. These negotiations aimed to reach a new agreement (as the previous one had expired) regarding the use, on Meta's platforms, of the musical works protected by SIAE. During the negotiation of this new Music Rights Agreement (MRA), SIAE repeatedly requested that Meta grant access to its economic data, so as to include in the agreement remuneration proportional to Meta's revenues derived from the use of such content, but the request proved unsuccessful.

At the outset of the investigation, AGCM considered Meta's conduct as an abuse of dominant position, which led the company, in the course of the proceedings, to submit a proposal for commitments. Some of these proposed commitments aimed at ensuring that negotiating counterparties receive the necessary data during the relevant negotiation cycles. After submitting the proposal to market testing, the Italian authority concluded that these commitments to share, during negotiations, the set of information defined therein constitute an essential step towards significantly reducing the imbalance that typically favors Meta *vis-à-vis* its negotiating counterparts. AGCM also considered that the sharing of the information listed in the commitments may constitute an essential element to ensure that future negotiations of the licenses covered by the commitments take place on a more balanced footing between the parties. Furthermore, the Italian authority held that the set of information identified in the commitments does not appear to be exhaustive and may be adapted – on the basis of transparent dialogue between the parties – to the specific needs of the negotiation in question, thereby addressing the authority's competition concerns.

The **Italian authority** also responded to the Questionnaire pointing to three additional cases that involved important data transparency issues, though they were brought in the

authority's consumer protection mandate.

In the first case, in the course of providing insurance placement services on behalf of the companies with which they had entered into distribution agreements for motor liability insurance policies, **Telepass S.p.A**. and **Telepass Broker S.r.l**. received information flows relating to the data of users requesting quotations, without those consumers being adequately informed[256]. The sharing of such information between companies within the Telepass Group and the insurance companies/intermediaries took place without prospective policyholders being properly informed of the collection and use of their data by the entities involved, including for commercial purposes[257]. Moreover, no information was provided to customers regarding the criteria or parameters used to select the proposed quotation[258].

As a result, the AGCM sanctioned the companies. On appeal, the *Consiglio di Stato* emphasized the importance of safeguarding personal data, stating that whenever questions concerning the processing of personal data within the competence of the Italian Data Protection Authority arise, closer cooperation between authorities is necessary[259].

In 2021, two more cases – one against **Google**[260] and the other against **Apple**[261] were concluded with the imposition of

256 Autorità Garante della Concorrenza e del Mercato (AGCM), 'Case no. PS11710 – TELEPASS/ACCORDO PRIMA ASSICURAZIONE, Provvedimento no. 28601' (9 March 2021) at <https://www.agcm.it/dotcmsCustom/tc/2026/3/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/1DA6D0AC5178B672C12586A00054EEF8/$File/p28601.pdf>. Accessed 30 March 2026.

257 Paragraph 50 of Decision no. 28601.

258 Paragraph 57 Decision no. 28601.

259 'Dati Personali E Protezione Dei Consumatori. Il Consiglio Di Stato Annulla La Decisione Del Tar Lazio Nel Caso Telepass' (Dejalex, 17 May 2024) at https://www.dejalex.com/2024/05/consiglio-di-stato-annulla-sanzione-telepass/#_ftn2.

260 Autorità Garante della Concorrenza e del Mercato (AGCM), 'Case PS 11147 – GOOGLE DRIVE-SWEEP 2017, Provvedimento n. 29890' (16 November 2021) at <https://www.agcm.it/dotcmsCustom/tc/2026/11/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/85F9DF40E1A8FEEEC125879C00500259/$File/p29890.pdf>. Accessed 30 March 2026.

261 Autorità Garante della Concorrenza e del Mercato (AGCM), 'Case PS 11150 – ICLOUD, Provvedimento n. 29888' (9 November 2021) at <https://www.agcm.it/dotcmsCustom/tc/2026/11/getDominoAttach?urlStr=81.126.91.44:8080/C12560D000291394/0/364118475

fines of €10 million on each company. Both companies engaged in two anticompetitive practices: one arising from information deficiencies, and the other from aggressive practices related to the collection and use of consumer data for commercial purposes.

Specifically, both at the phase of account creation – which was indispensable for accessing all the services offered – and during the use of the services, Google omitted relevant information necessary for consumers to make a conscious decision to accept Company's collection and use of their personal data for commercial purposes. Moreover, during the account creation phase, Google pre-imposed user's acceptance to the transfer and/or use of their data for commercial purposes. This pre-activation enabled the transfer and use of data by Google without the need for subsequent stages in which users could confirm or modify the choice pre-set by the company.

Apple, in turn, both during the creation of the Apple ID and when accessing the Apple Stores (App Store, iTunes Store and Apple Books), did not provide users with explicit and immediate information regarding the collection and use of their data for commercial purposes, highlighting only that data collection was necessary to enhance the consumer experience and the use of services. In addition, Apple's promotional activities relied on a method of obtaining consent for the use of user data for commercial purposes without providing consumers with the possibility to make an express choice regarding the sharing of their data. This consent architecture designed by Apple did not allow users to exercise their will concerning the commercial use of their data. Consequently, consumers were conditioned in their consumption choice and subjected to the transfer of personal information, which Apple could have for its promotional purposes in various ways[262].

1A82355C125879C00500255/$File/p29888.pdf>. Accessed 30 March 2026.

262 Autorità Garante della Concorrenza e del Mercato (AGCM), Press Release. 'PS-11147-PS11150 - ICA: $20 million sanctions against Google and Apple for commercial use of

(viii) Data use prohibition

Definition

This remedy may largely overlap with the concept of data segregation, with the latter being an infrastructural arrangement that ensures the effective application of the former. However, the two do not necessarily go hand in hand, as the prohibition to use data for some specific purpose (as those relating to third party obligations in the European Data Act, for instance) can also be implemented through other technical solutions, such as labeling and contractual commitments.

Application

United Kingdom

The **Competition and Markets Authority** (CMA) adopted a decision involving data use prohibition remedies in the **Google's Privacy Sandbox**[263] case. In 2021, the CMA opened an investigation into Google's proposal to remove third-party cookie (TPC) functionalities from the Chrome browser and replace them with a suite of "Privacy Sandbox" tools. TPCs play a crucial role in digital advertising because they allow companies to target advertising more effectively, although they also raise significant privacy concerns. Google introduced the Privacy Sandbox project as a set of new ad-targeting tools designed, according to the company, to improve user privacy within its browser. Complaints regarding the proposed tools were submitted primarily by newspaper publishers, publisher associations, and competing technology firms, which alleged that the changes could undermine the ability of other firms to generate revenue from digital advertising[264].

user data' (26 November 2021) at <https://en.agcm.it/en/media/press-releases/2021/11/PS-11147-PS11150>. Accessed 30 March 2026.

263 The relevance of this case was highlighted by the authority in its response to the Questionnaire.

264 Competition and Markets Authority (CMA), 'Investigation into Google's 'Privacy Sandbox' browser changes' (8 January 2021, last updated 17 October 2025) at <https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-change>. Accessed 30 March 2026.

According to the CMA, the Privacy Sandbox proposal raised a number of competition concerns, including the risk of Google self-preferencing its own advertising inventory and ad-tech services by transferring key functionalities into Chrome, thereby enabling Google to influence digital advertising market outcomes through Chrome in a manner that would not be open to third-party scrutiny, creating conflicts of interest. In addition, the proposal could allow Google to exploit its dominant position by limiting Chrome users' ability to choose how their personal data is used for advertising purposes. In 2022, the CMA accepted Google's commitments that included, in particular,

> (i) a commitment not to combine user data from certain specified sources for the purposes of targeting or measuring digital advertising on either Google owned and operated ad inventory or third-party inventory; and
>
> (ii) a commitment not to design any of the Privacy Sandbox Proposals in a way which could self-preference Google, not to engage in any form of self-preferencing practices when using the Privacy Sandbox technologies and not to share information between Chrome and other parts of Google which could give Google a competitive advantage over third parties[265].

It is worth noting that, in this case, the CMA relied extensively on consultation with the Information Commissioner's Office

265 Competition and Markets Authority (CMA), 'Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals, Case number 50972' (11 February 2022) at <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf>, p. 55. The commitments were quite detailed, requiring Google also to: (i) ensure that the CMA's role and the ongoing CMA process are mentioned in Google's key public announcements; (ii) instruct its staff not to make claims to customers which contradict the commitments; (iii) report regularly to the CMA on how Google has taken account of third party views; (iv) address concerns about Google removing functionality or information before the full Privacy Sandbox changes, including by delaying enforcement of its Privacy Budget proposal, and offering commitments around the introduction of measures to reduce access to IP addresses; (v) clarify the internal limits on the data that Google can use; (vi) provide greater certainty to third parties developing alternative technologies; (vii) improve the provisions on reporting and compliance, including by appointing a CMA-approved monitoring trustee; and (viii) provide for a longer duration of 6 years from the date of any decision to accept Google's modified commitments.

(ICO) regarding privacy and data-protection issues. As expressly stated in paragraph 18 of the commitments, "Google acknowledges that the CMA will involve the ICO to achieve the Purpose of the Commitments as agreed between the CMA and the ICO and subject to applicable legislation. The CMA was tasked to consult the ICO before issuing any notification [to Google that competition law concerns remain such that the Purpose of the Commitments will not be achieved]".[266]

In April 2025, however, Google announced that it would not implement a new standalone prompt for third-party cookies, reiterating instead that users could continue to decide whether to enable or disable such cookies according to their preferences. Following this announcement, the CMA launched a public consultation on whether Google should be released from its existing commitments and in October 2025, the authority determined that there were reasonable grounds to conclude that the competition concerns previously identified no longer applied, and that Google should accordingly be released from its commitments[267].

Finally, it is worth mentioning another case brought by the **CMA,** stemming from the **Meta** (formerly Facebook) investigation launched in 2021, which concerned competition issues arising from the company's use of data obtained when providing digital advertising services[268]. The investigation examined whether Meta had abused its dominant position in the market for digital display advertising (DDA) by using data collected through its advertising activities and its single sign-

266 Competition And Markets Authority (CMA), 'Case 50972 - Privacy Sandbox, Google Commitments Offer' (4 February 2022) at <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf>. Accessed 30 March 2026.

267 Competition and Markets Authority (CMA), 'Decision to release commitments previously accepted by the CMA in respect of Google's Privacy Sandbox Proposals' (17 October 2025) at https://assets.publishing.service.gov.uk/media/68f213ce06e6515f7914c728/Decision_to_release_the_commitments_previously_accepted_by_the_CMA_in_respect_of_Google_s_Privacy_Sandbox_proposals.pdf.

268 The relevance of this case was highlighted by the authority in its response to the Questionnaire.

on system (*Facebook Login*) to advantage its own services in adjacent markets (namely, *Facebook Marketplace,* an online classified advertising service) to the detriment of competitors. In May 2023, Meta submitted a set of commitments to address the CMA's concerns[269].

Following a public consultation on these proposed commitments, the CMA decided to accept them in November 2023. Among the commitments, Meta undertook to allow advertising customers to opt-out of having their relevant advertising data used by Meta to operate or improve the Facebook Marketplace service. Beyond Marketplace, Meta also committed to limiting its use of advertising data derived from digital display advertising and business tool services that identify advertisers. Moreover, Meta agreed to implement necessary measures to ensure that employees involved in product development do not use such information to design or improve Meta's products in competition with advertisers[270].

United States of America

Another case involving data use prohibition is the already mentioned **US DC Circuit District Court** decision in **United States v. National Association of Realtors** (2020)[271]. The DOJ alleged that NAR policies impeded competition between brokers, disadvantaged discount and non-traditional brokerage models, limited transparency for home buyers and sellers, and restricted how MLS data could be displayed or used by competing platforms and business models. The DOJ

269 Competition and Markets Authority (CMA), 'CMA protects competition by curbing Meta's use of ad customers' data' (3 November 2023) at <https://www.gov.uk/government/news/cma-protects-competition-by-curbing-metas-use-of-ad-customers-data>. Accessed 30 March 2026.

270 Competition and Markets Authority (CMA), 'Decision to accept binding commitments offered by Meta on its use of data obtained through digital display advertising', Case AT 51013' (3 November 2023) at <https://assets.publishing.service.gov.uk/media/6543a5b7d36c-910012935c7a/Meta_Final_Commitments_Decision_final.pdf>. Accessed 30 March 2026.

271 See <https://www.justice.gov/atr/case/us-v-national-association-realtors-0>. Accessed 30 March 2026.

identified several competitive concerns, including MLS rules that allowed brokerages to withhold commission information from prospective buyers, policies that enabled steering away from lower-commission listings, and restrictions preventing consumer-facing websites from displaying complete listing data. These practices were viewed as reinforcing traditional commission structures, suppressing emerging digital brokerage models, and reducing consumers' ability to compare pricing. The rules collectively reduced price competition, discouraged innovation in brokerage service formats, and prevented market participants and consumers from accessing crucial information embedded in MLS systems.

The DOJ submitted a proposed consent judgment that would have imposed several pro-competitive reforms on NAR's rules. Pursuant to the proposal, the settlement prohibited brokers from advertising their services as "free" when MLS data indicated that compensation was being paid through seller-funded commissions. This remedy targeted situations in which existing data about commission flows was used to misrepresent cost to consumers, thereby distorting competitive comparison. By preventing the use of MLS compensation data to imply zero-priced services, the obligation aimed to improve accuracy in market signaling, reduce consumer deception regarding brokerage costs, and support competitive entry from firms seeking to differentiate on price[272].

In the **US District Court for North Carolina's** case **United States v. RealPage, Inc. et al (2025)**[273], the DOJ challenged RealPage's conduct in the market for algorithmic revenue-management software used by large landlords in U.S. residential housing. RealPage's core product aggregated competitively

272 It should be noted that in July 2021 the DOJ withdrew from the settlement before it was submitted for judicial approval, invoking its authority to reassess the competitive implications of NAR's policies. As a result, none of the proposed obligations effectively entered into force, and the agency resumed its broader investigation into NAR's conduct and the parties are still litigating in 2025.

273 See <https://www.justice.gov/opa/pr/justice-department-requires-realpage-end-sharing-competitively-sensitive-information-and>. Accessed 30 March 2026.

sensitive rental data from landlords and produced automated pricing recommendations that many property managers followed when setting rents.

The DOJ alleged that RealPage's data aggregation and algorithmic coordination suppressed price competition among landlords, facilitated parallel rent increases, and distorted competitive dynamics in residential rental markets. The DOJ identified several competitive concerns, including RealPage's collection of real-time, non-public pricing and occupancy data from competing landlords; its use of that data to generate unified pricing recommendations; and contractual restrictions that discouraged property managers from deviating from algorithmic outputs. These practices allegedly produced a form of "algorithmic collusion" by centralizing sensitive rental information and distributing coordinated pricing guidance. According to the DOJ, RealPage's system reduced independent price-setting, raised rents, and impaired competition from landlords who were not part of the RealPage network. The agency concluded that RealPage's conduct materially increased market rigidity, limited competitive responses to excess supply, and created structural barriers that prevented rivals from competing on data scale.

In February 2025, the DOJ announced a proposed consent decree (with a 3-year monitoring trustee) that would impose significant behavioral constraints on RealPage's future data practices[274]. The agreement was designed to disentangle pricing decisions from the shared data infrastructure RealPage created. Pursuant to the proposed consent, data use prohibition remedies were included so RealPage may not use current or historical non-public data belonging to individual property owners while any software that generates prices or pricing recommendations for rental properties runs, including in any software or service that generates prices or pricing

274 See <https://www.justice.gov/opa/pr/justice-department-requires-realpage-end-sharing-competitively-sensitive-information-and>. Accessed 30 March 2026.

recommendations for rental properties for modeling training purposes. RealPage should also not use any models trained on non-public data belonging to individual property owners in software that generates prices or pricing recommendations for rental properties.

The RealPage settlement is part of a broader context, since the action was actually brought by the DOJ and nine attorneys general not only against RealPage, but also against major landlords in the United States — Greystar, Camden, Cortland, Cushman & Wakefield/Pinnacle, LivCor, and Willow Bridge — for violations of the Sherman Act[275]. Specifically with respect to Greystar (*Greystar Management Services LLC*), the allegation was that the company (along with the other parties) was sharing competitively sensitive data to coordinate price recommendations using algorithms developed by RealPage. In August 2025, the DOJ reached proposed settlement to resolve the charges against Greystar, under which the company is prohibited from (i) using any anticompetitive algorithm that generates pricing recommendations based on sensitive competitive data from its rivals or that incorporates certain anticompetitive features, and (ii) sharing commercially sensitive information with competitors[276].

India

Another case involves the **Competition Commission of India (CCI)**'s investigation launched in 2021 against **WhatsApp's privacy policy**, concluding that the platform users should accept the changes or risk losing access to the platform. In 2024, the CCI imposed a five-year ban on WhatsApp sharing

275 United States and State of North Carolina v RealPage, Inc, 'Amended Complaint, Case No 1:24-cv-00710-LCB-JLW' (MDNC, 1 July 2025) at <https://oag.ca.gov/system/files/attachments/press-docs/U.S.%20et%20al.%20v.%20RealPage%2C%20Inc.%20-%2047%20-%20First%20Amended%20Complaint.pdf>. Accessed 30 March 2026.

276 United States Department of Justice, 'Justice Department Reaches Proposed Settlement With Greystar, Largest U.S. Landlord, to End Its Use of Anticompetitive Algorithmic Pricing', Press Release (8 August 2025) at <https://www.justice.gov/opa/pr/justice-department-reaches-proposed-settlement-greystar-largest-us-landlord-end-its>. Accessed 30 March 2026.

user data with other Meta entities for advertising purposes – a data use prohibition remedy – and fined the company US$25.4 million for abusing its dominant position.

WhatsApp challenged the decision, and in November 2025, the appellate court (National Company Law Appellate Tribunal) lifted the data-sharing ban[277] stating that "we note that this remedy is contestable as the rationale for the duration of five years ban was missing altogether in the Impugned Order. The justification that such a period would 'revive competitive conditions' cannot meet the threshold required by law as claimed by the Appellants"[278]. Nevertheless, the court maintained the fine[279].

Greece

In Greece, the antitrust authority – the **Hellenic Competition Commission** (HCC) – reported that it has imposed data remedies in its decision n^{0}. 775/2022[280] concerning a merger notification, pursuant to Article 6 of Law 3959/2011. The concentration notification concerned the **acquisition of sole control by Delivery Hero SE** ("Delivery Hero") **over Alfa Distributions S.A., Inkat SA, Delivery I.K.E. and E-Table I.K.E.** ("E-Table").

At the time, Delivery Hero operated the largest and most popular food delivery platform (e-food.gr) while E-Table operated the platform e-table.gr that offered restaurant

277 Reuters, 'India tribunal lifts WhatsApp data-sharing ban, upholds Meta fine' (4 November 2025) at <https://www.reuters.com/sustainability/boards-policy-regulation/india-tribunal--lifts-whatsapp-data-sharing-ban-upholds-meta-fine-2025-11-04/>. Accessed 30 March 2026.

278 National Company Law Appellate Tribunal (NCLAT), 'Competition Appeal No. 1 of 2025 & Competition Appeal No. 2 of 2025, Judgment' (4 November 2025) p. 164 at <https://nclat.nic.in/display-board/view_order>. Accessed 30 March 2026.

279 National Company Law Appellate Tribunal (NCLAT), 'Competition Appeal No. 1 of 2025 & Competition Appeal No. 2 of 2025, Judgment' (4 November 2025) p. 182 at <https://nclat.nic.in/display-board/view_order>. Accessed 30 March 2026.

280 Hellenic Competition Commission (HCC), Decision 775/2022 - Clearance of the notified concentration under ref. no 8003/1.10.2021 (18 April 2022) at <https://www.epant.gr/en/decisions/item/2938-decision-775-2022.html>. Accessed 30 March 2026. The relevance of this case was highlighted by the authority in its response to the Questionnaire.

reservation services (e.g. consumers were able to reserve a table to their preferred restaurant through e-table.gr). One of HCC concerns was that the combination of consumers data collected from the new entity's platforms, e-food.gr and e-table.gr, would allow it to implement personalized promotion strategies, thereby giving the new entity a competitive advantage to such a degree that its competitors would no longer be able to compete it effectively.

To address this concern, Delivery Hero committed to not to use end-user data collected from its food delivery platform (e-food.gr) in order to implement personalized promotion strategies for services offered by the acquired platform (e-table.gr) and vice versa, unless consumers have previously provided their consent to receive personalized advertising and marketing communications, in accordance with existing data protection rules. Moreover, the decision stipulated that Delivery Hero is prohibited from integrating the e-table and e-food platforms for a period of one year from the issuance of the decision. Following this period, although integration may take place, Delivery Hero is required, for an additional year, not to use the data of e-food platform end users to implement targeted promotional strategies for e-table services, and vice versa. The sole exception, as previously noted, arises where end users have provided prior consent to receive personalized advertising, in accordance with applicable data protection legislation. Consequently, the commitments undertaken by Delivery Hero effectively constitute a set of overlapping remedies, encompassing data segregation, data use prohibition and data control enhancement mechanisms.

(ix) Data anonymization

Definition

Data anonymization is a remedy that creates an obligation to the process of turning personal data into anonymous information so that a person is no longer identifiable. This is a type of remedy that has not yet been applied in isolation. For that reason, some argue that this may be a sign that this remedy alone may not be sufficient to address competitive concerns by itself, being necessary to combine it with additional measures to reach its desired effects on competition.

The main challenge in the implementation of this type of remedy concerns the measures that are considered to be sufficient to ensure effective anonymization. This is particularly concerning because, with technological advancement, the ability of attackers to reidentify individuals in a supposedly anonymized dataset increase. As a result, it is important that competition authorities keep abreast of technological developments and are able to enforce the use of the most modern anonymization techniques.

Achieving this may be challenging, so one approach that has been recommended for anonymized data sharing (and specifically for article 6 (11) of the DMA)[281], and that is in line with technological neutrality, is the one of K-anonymity. This approach ensures that users cannot be distinguished from k-1 other users by ensuring that no record in a dataset represents fewer than k users, thus preserving the value of the data while minimizing the risk of reidentification. This can be achieved in multiple ways, either by generalizing data or suppressing data, or a combination of the two. To do that, competition authorities may be required to become more conversant with data science techniques in order to ensure that the anonymization is done at the correct abstraction level that allows them to achieve the remedy's purpose while also maintaining the scope of the remedy to what is proportionate to that end.

281 Filippo Lancieri, Laura Edelson, Inge Graef". Access to Data and Algorithms: For an Effective DMA and DSA Implementation", CERRE report (March 2023).

Application

European Union

One example of a data anonymization remedy is provided by the DMA in its article 6 (11), which requires gatekeepers to share with any third-party providing online search engine services, upon request, "access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines".

Therefore, in the context of DMA enforcement, it is worth recalling the specification proceedings previously mentioned, initiated by the **European Commission** in 2026, which remain pending a final decision, in relation to Google. One of the set of proceedings specifically concerns the obligation set out in Article 6(11) of the DMA, focusing on "the scope of data, the anonymization method, the conditions of access, and the eligibility of AI chatbot providers to access the data"[282]. The Commission's action seeks to guide Google in complying with the obligation imposed by the DMA.

United States

Another illustration of a data-anonymization remedy can be found in the decision of the **United States District Court for the District of Columbia** in the case against **Google**. In that instance, judge Metah required the implementation of a range of privacy-enhancing techniques, which included k-anonymity, with the aim to mitigate privacy risks associated with the sharing of datasets. Notably, the remedy refraining from prescribing a specific technical solution and instead delegated this assessment to a Technical Committee responsible for

282 European Commission, 'Digital Markets Act: Commission opens proceedings to assist Google in complying with interoperability and online search data sharing obligations under the Digital Markets Act', News Announcement (26 Jan 2026) at <https://digital-markets-act.ec.europa.eu/commission-opens-proceedings-assist-google-complying-interoperability-and-online-search-data-sharing-2026-01-27_en>. Accessed 30 March 2026.

overseeing its implementation. The court decision underscores that the effective implementation of anonymization techniques related to user-side data constitutes an important and particularly challenging component of the remedy package.

(x) Data disgorgement

Definition

The idea of disgorgement of data that was illegally collected or curated is closely related to the concept of algorithmic destruction or disgorgement. The gist of the remedy is that the offending training data and its effects are removed from the existing model, making it as if that data was never used in the first place.

It is important to highlight that this remedy has been used so far only in the context of privacy violations[283], but there seems to be no reason why it cannot be applied for antitrust cases as well.

Application

United States

One must recognize that disgorgement is easier said than done, particularly if it does not only require the expungement of illegally-gotten data from the records, but also the erasure of the algorithms trained with that data, as argued by one **FTC** Chairwoman[284]. Not surprisingly, the remedy has so far been imposed by the FTC only **in settlements,** listing it as one of the necessary conditions to pursue the case through litigation, rather than being enforced through a specific order like cease-and-desist or injunctions[285].

283 Hutson, Jevan and Winters, Ben, America's Next 'Stop Model!': Model Deletion (September 20, 2022). Georgetown Law Technology Review. The mentioned cases are: In the Matter of Everalbum; In the Matter of Cambridge Analytica; USA v. Kurbo Inc. and WW International; FTC v. Ring; and USA v. Edmodo.

284 Rebecca Kelly Slaughter, Acting Chairwoman, FTC, Protecting Consumer Privacy in a Time of Crisis (Feb. 10, 2021), <https://www.ftc.gov/system/files/documents/ public_statements/1587283/fpf_opening_remarks_210_.pdf>. Accessed 30 March 2026.

285 Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as The FTC's Newest Enforcement Tool for Bad Data*, 29 RICH. J.L. & TECH. 1 (2023).

It has also been speculated that it is unlikely that the remedy could be imposed through a preliminary injunction, since it relates to a harm that has already happened, and it is hard to verify that the algorithm no longer uses certain data (which has usually been fed in anonymized or combined form)[286]. In this light, it is argued that deletion of the algorithm is the only way to ensure the removal of privacy harm, as they could continue even if their individual data is no longer distinguishable or in active use by that algorithm[287]. It has also been argued, however, that algorithmic deletion should only be ordered for the most blatant violations, and not when data has become stale for the passage of time[288].

The main challenge when it comes to implementation is relating to the technical measures used to ensure destruction. For instance, in the same way that destroying data from the physical copies or the hard drive of a computer may not be sufficient if there is a back-up somewhere that can be used in making future choices, there could still be significant effects in the provision of products and services in the market if the data has been used to inform the developments of certain features of the algorithm that do not reveal such a characteristic. Therefore, due diligence procedures can be followed to provide more guarantees of compliance with the principles underlying destruction/disgorgement[289].

Another key challenge pertains to the proportionality analysis of data disgorgement remedies: where a dataset is only in part the result of illegal conduct, how to assess whether destruction is appropriate? When is the transfer of such data

286 Id. , p. 33-34

287 Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. REV. 479, 502–03 (2022).

288 Srikaran, V., 'Beyond Data Deletion: Addressing Anticompetitive Conduct in the Era of Machine Learning', 20 Wash. J.L. Tech. & Arts 1 (2025).

289 Such as: (i) reviewing an independent audit of a disposal company's operations; (ii) obtaining information about the disposal company from several references; (iii) requiring that the disposal company be certified by a recognized trade association; (iv) reviewing and evaluating the disposal company's information security policies or procedures. See <https://www.ftc.gov/business-guidance/resources/disposing-consumer-report-information-rule-tells-how>. Accessed 30 March 2026.

to another competitor, rather than destruction, a more suitable option? And how do the balance of interests of third parties (particularly consumers, competitors, and society as a whole) weigh in this proportionality analysis? Once again, we do not intend to answer those questions, but only highlight them to allow further discussions in the future.

(8) LESSONS LEARNED AND WAY FORWARD

Data occupy a distinctive position in contemporary competition assessment, being simultaneously (i) an economic asset that can be monetized and traded; (ii) a strategic input that shapes product quality, targeting and algorithmic performance; (iii) an infrastructural resource that is replicable and can support multiple downstream uses; and (i) an object regulated under multiple legal regimes, notably competition, data protection, consumer protection, sectoral regulation and, frequently, intellectual property and cybersecurity.

This multi-dimensionality explains why data remedies are not a homogeneous toolbox. International practice confirms that their design must vary with the nature of the market (and the role data play within it), the type of market power exercised (control over datasets, gateways or rules), the degree of regulatory interdependence (where feasibility depends on privacy, security or sector-specific constraints), and the risk of unintended and spillover effects (including privacy degradation, dampened investment incentives, facilitation of collusion, or strategic circumvention). The central lesson is therefore to treat data remedies as targeted instruments to restore contestability where data operate as a reinforcing competitive lever, and where spillover effects can be minimized.

In this report, we have examined different types of data remedies, which can be grouped into three categories related to their core functions:

(1) Remedies that enhance control and transparency, which address harms that rely on opacity and asymmetric information. Data transparency measures directed to regulators for audit and scrutiny, or to users and business partners to clarify rules, criteria and consequences of data processing can constrain discretionary governance and reduce the scope for discriminatory treatment and self-preferencing. Data control enhancement measures,

including more granular and neutral choice architectures or governance mechanisms that rebalance decision-making over processing, respond to harms linked to exploitative terms and exclusionary leveraging through cross-use of personal data. Their competition rationale is to reduce lock-in and prevent data processing choices (defaults, bundling, or design nudges) from becoming foreclosure tools that entrench network effects.

(2) **Remedies that facilitate data mobility and contestability**, which focus on switching costs and scale advantages. Data portability can weaken lock-in by enabling users (or authorized third-parties) to transfer relevant data in usable formats, thereby supporting entry and multi-homing. Yet portability often remains "lightweight" unless accompanied by technical standards, service-to-service tools and reliable commitments that preserve data utility. Interoperability tackles the technical and governance conditions for systems to communicate and services to coexist; it is particularly apt where harms arise from network effects and ecosystem leveraging, including refusal, degradation or delay in providing interfaces. Data access and sharing obligations are the most intrusive instruments in this category, justified primarily where competitive harm is rooted in input foreclosure or self-reinforcing feedback loops and where access to high-quality, timely datasets is necessary to reach a minimum viable scale. Their legitimacy depends on disciplined scoping and governance so that access restores competition without becoming an indefinite subsidy, while also preserving the privacy and data protection of any involved individuals.

(3) **Remedies that restrict, segregate or eliminate power coming from data processing**, which are aimed at preventing the leveraging of informational advantages across markets. Data segregation and data use prohibitions target self-preferencing and exclusionary conduct that depends on internal information advantages—such as the use of non-public business user data to compete against business users, or the combination of sensitive datasets to reinforce dominance in adjacent layers. Data anonymization and privacy-enhancing technologies (PETs) are often enabling constraints that make other remedies feasible by reducing

reidentification and misuse risks. Data disgorgement is exceptional, but conceptually important: it seeks to neutralize advantages that cannot be undone through forward-looking constraints alone, particularly where unlawful accumulation of data has durable competitive effects.

Clearly, each of these categories presents its own challenges. However, we also find similarities across them, especially as they are better seen as dots along a continuum, rather than compartmentalized types of remedies.

For instance, data transparency may be considered a first step towards guaranteeing effective protection and autonomy of the customers of an undertaking, which can be improved by providing concrete mechanisms to enhance controls. Data portability is the next step of that and represents the connection ring between customer-facing and competitor-facing remedies, such as data sharing, which are designed to tilt the scale in favor of competitors in order to restore competition. Progressing to the third stage, remedies that are focused on preventing data power through destruction or restrictions of processing go one step further than simply putting a thumb on the scale, as they hinder the undertaking from operating at full capacity with its data processing capabilities.

Furthermore, regulators may mix and match some of these remedies to accentuate and complement their effects, as was visible with the complex remedy package adopted by judge Mehta in the Google litigation in the United States of America.

In terms of challenges, experience across jurisdictions highlights that some remedies depend on user behavior in ways that can undermine effectiveness. Portability and user-control measures assume comprehension, engagement and willingness to switch; in practice, behavioral biases, choice complexity and strong network effects may prevent these remedies from delivering structural change. Interoperability poses the opposite problem: it can be technically complex, dynamic and vulnerable to strategic degradation, requiring continuous updates, quality-of-service parameters and credible dispute resolution. Data access and sharing raise free-riding risks and require difficult choices on remuneration, duration and the granularity of disclosure, especially in markets where the value of data is time-sensitive and refreshed continuously.

These challenges are compounded by legal and institutional tensions. Intellectual property and trade secrets do not preclude access, but they require

safeguards (confidentiality protections, limited-purpose licenses, auditability and, where appropriate, technical minimization) to avoid unnecessary exposure of proprietary elements. Data protection law introduces hard constraints when remedies involve personal data, including the requirements of lawful basis, purpose limitation, minimization and accountability. Conditioning remedies on consent may preserve legality but may also reduce effectiveness where fully informed consent is not realistically obtainable, or where consent flows can be manipulated. Conversely, grounding sharing on the existence of a legal obligation or legitimate interests in data processing may address one layer of lawfulness while leaving uncertainty over recipients' downstream processing. Monitoring and enforcement remain decisive: behavioral and information-intensive remedies confront persistent asymmetries of information, making trustees, technical experts, reporting obligations, KPIs and audit rights valuable—to the extent that mandates are precise, time-bounded, and respectful of confidentiality and due process. Underlying all of this is proportionality: overly broad remedies can chill innovation and undermine privacy; while overly narrow remedies can be ineffective, leaving durable data advantages intact.

Data remedies, more frequently than not, transcend traditional competition law boundaries because they operate on resources regulated for additional objectives, including fundamental rights, consumer autonomy, sectoral integrity and cybersecurity. Effective design and implementation therefore may require structured coordination with data protection authorities, sectoral regulators and consumer protection bodies.

In this regard, European case-law provides a practical template: competition authorities may take account of data protection compliance as part of the competitive assessment where relevant to identifying abnormal methods of competition and consumer harm; however, they do not substitute themselves for data protection supervisory bodies. Where competition decisions depend on determinations that hinge on data protection concepts, the principle of sincere cooperation[290] supports a duty to consult the competent supervisory authority,

290 As mentioned above, the principle of sincere cooperation requires the Union and the Member States to work together, in mutual respect, to carry out obligations arising from the Treaties (Art. 4(3) TEU). Member States must adopt all appropriate measures, whether general or specific, to ensure compliance with these Treaties' obligations, to support the Union in achieving its objectives, and to avoid actions that could undermine these objectives. The significance of this principle is highlighted in the ECJ's judgment in case C-252/21, *Meta Platforms Inc v. Bundeskartellamt*. The ECJ has clarified that a national public authority consulted by another must respond to requests for information within a reasonable time, either by providing the requested data and clarifications or by indicating whether it intends to initiate an investigation under the relevant regulatory framework. If no response is given within a reasonable period, the consulting authority, such as the Bundeskartellamt in that case, the consultant may proceed with its investigation (See paragraphs

avoid conflicting interpretations, and ensure coherence. Coordination should thus be understood as functional complementarity—clear division of mandates combined with operational alignment—rather than institutional overlap.

Drawing from past experience, one must stress the importance of a case-by-case analysis and calibration of those remedies, ensuring that they are anchored on specific theories of harm and take into consideration how data functions in the market (input, asset, infrastructure), including the role of network effects and scale.

With regard to the implementation of specific remedies, additional highlights can be made following the presented review of cases:

(i) **Data portability** remedies should come with limitations regarding their possible effects on trade secrets and other legitimate interests of third parties. However, as noted by the Article 29 Working Party, the result of those considerations should not be a refusal to provide all information: rather, an appropriate balancing ought to be made on the basis of the magnitude and probability of the risks involved. One important distinction that may also be relevant at the balancing stage is that between two forms of portability: download and direct transfer. Standard-setting can facilitate the effectiveness of the latter[291], but it is also important to ensure that rules are established in a way that does not lead to entrenchment of market power by incumbents. Reporting mandates with the inclusion of stakeholders into testing of tentative portability solutions[292], habilitation of specialized third parties and transparency over the settling of technical problems[293] seems to help in that regard.

(ii) **Interoperability remedies** raise complex technical questions - for instance regarding feasibility and security, and other ordinary commercial restrictions- and may need the support of independent trustees to ensure monitoring. This should not imply, however, a delegation of competences of the enforcer, for an indefinite period

58 and 59 of the ECJ's decision, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:-62021CJ0252)>. Accessed 30 March 2026.

291 As foreseen by legislation in the EU and Brazil, for instance.

292 As done in CADE's case against Bradesco and in AGCM's decision against Google as done in CADE's case against Bradesco and in AGCM's decision against Google.

293 As proposed by the Competition and Markets Authority under the DMCCA.

of time, and entirely at the costs of the undertaking[294]. An alternative that may be used to increase effectiveness is assigning an asset to an independent third party, as was done in the *Cisco/Tandberg* merger decision by the European Commission. Effectiveness is also enhanced by transparency mandates over available features and the process of interoperability management, as well as the use of dispute resolution mechanisms and the need to future-proof the remedy against possible technological evolution[295]. Important questions may arise on the allocation of costs relating to the implementation of interoperability mandates, revealing the importance of defining first principles (for instance, FRAND and eventual caps to the frequency of API calls) in the remedy itself.

(iii) **Data segregation** remedies often imply firewalls between different lines of business and tend to be more credible when parties commit significant resources to educating staff about the requirements of the measures and supporting them with disciplinary procedures and independent monitoring. Their effectiveness can be increased when the scope encompasses not only personally identifiable data, but also any inferences derived from the processing of certain data. It can also be useful to include restrictions on undue influence by executives that do not belong to that particular business line over the rules and standards for the processing of the data that is subject to the remedy[296].

(iv) **Data access/sharing** remedies require careful balancing between the need to provide access and the incentives for ex-post appropriability. In that regard, one should take into account that the latter incentives may be weaker when the data at issue is only a byproduct of a company's operation and not a key asset to guarantee returns on investment. However, the broader a mandated disclosure and the more it affects an asset that is crucial to the business model of the firm (up to the point in which it is tantamount to a divestiture), the closer must the data

294 As learned in the first EU *Microsoft* case.

295 As noted in the DMA case concerning Apple, and to some extent in the EU decision in *Meta/Kustomer.*

296 As learned in the Hungarian competition authority's decision on *General Logistics Systems/iLogistics*.

be connected with the violation at stake[297]. At the same time, important challenges must be resolved around the legitimacy of data processing by third parties, suggesting that transparency and purpose limitation should be at the center of the design of such remedies[298]. Proposed alternatives to imposing the establishment of mechanisms for outright data transfers may be the requirement to bilaterally negotiate access conditions[299] , the use of sandboxes and the provision of *in-situ* data rights.

(v) **Data control enhancement** remedies ensure that decisions over data processing are done (either by data subjects, or by undertaking affording more granular control over further uses of data for which collection has been authorized. This can be done through control panels[300] or through the provision of clearer choice options[301]. It should be noted that the involvement of data protection authorities in the design of these remedies may lead to the adoption of options permit to increase the data protection safeguards beyond the minimum level[302].

(vi) **Privacy Enhancing Technologies (PET)** remedies require the application of technologies that preserve privacy and anonymity. On this front, it seems important both to have technical committee to recommend resasonable data security standards, and to consult with the concerned undertaking and affected parties who might have more in-depth knowledge of the industry[303].

(vii) **Data transparency** remedies specify details under which a firm must make disclosures to its customers or to the regulator, with a view to reducing the scope for discretion and abusive application of its rules and standards. One frequent issue is sufficiently detailed information regarding the application of rules to concerned undertakings, including any necessary training of staff to make

297 As ruled in the US *Google* remedy decision.

298 As Illustrated by the GDF Suez decision by the French competition authority.

299 As happened in the Deutsche Bahn decision by the Bundeskartellamt.

300 As in the Facebook decision by the German competition authority.

301 As done in the Bundeskartellamt's case Against Google.

302 As noted by the Italian data protection authority in the *Apple ATT* case.

303 As per the decision in the Google remedy case by judge Mehta.

that understandable[304], notifications regarding updates to such rules, and regular reporting over complaints and dispute resolution procedures[305]. Furthermore, the remedy can act as a complement to ensure the effectiveness of other remedies, by requiring the firm to proactively and sufficiently inform their beneficiaries[306].

(viii) **Data use prohibition** remedies imply the application of governance measures that prevent the use of data in a particular way, without limiting themselves to restricting their transfer or access as done in data segregation remedies. For instance, they may require that the rules for data processing do not involve any use for a particular purpose[307], self-preferencing[308], the sharing of sensitive information with competitors, or the use of sensitive information for personalization[309], recommendation algorithms or model training[310].

(ix) **Data anonymization** remedies can be subsumed to some extent into PET remedies, but they concern one specific type of intervention as they are aimed to prevent reidentification of individuals or entities in a dataset. Since anonymity is imperfect and the techniques used may have different impact on the utility of a dataset, a remedy may prescribe the level of anonymity (for instance, based on K-anonymity) that is appropriate in one or more specific situations.

(x) **Data disgorgement** remedies require deletion of data, while also calling for a reflection on the flanking measures to prevent such data from being resurrected through technical measures or inferences based on correlated datasets or algorithms. It is also important to carefully assess the proportionality of such orders, including in particular the impact on the undertaking's business and the possible effects that such destruction may have.

304 As provided in the remedy concerning the *Google Ad* case by the Authorité de la Concurrence.

305 As learned, among other cases, from the Google Ad case in France, the DMA case against Apple and the DCMCCA case against Google.

306 As occurred in the remedy adopted in the European Commission's case against Amazon.

307 As required by the Indian decision in the case against WhatsApp.

308 As was the case in the *Google Privacy Sandbox* commitment made to the CMA.

309 This was a concern in the HCC's *Delivery Hero/ Alfa Distributions* merger decision.

310 As established in the US DOJ's remedy against Realpage.

Lastly, it is important to bear in mind that data remedies are not ends in themselves. Their institutional objective is to restore and preserve contestability, protect consumers through meaningful choice and quality, and sustain incentives for innovation in data-driven markets. Achieving this will require greater technical sophistication in remedy design and supervision, and deeper interinstitutional cooperation to ensure coherence across competition, data protection, consumer and sectoral frameworks.