RSC 2023/30
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

WORKING PAPER

Shall we share?
The principle of FRAND in B2B data sharing

Marco Botta

European University Institute
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

Shall we share?
The principle of FRAND in B2B data sharing

Marco Botta

RSC Working Paper 2023/30

ISSN 1028-3625

Published in April 2023 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy

With the support of the Erasmus+ Programme of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Robert Schumann Centre for Advanced Studies
The Robert Schuman Centre for Advanced Studies (RSCAS) was created in 1992 and is currently directed by Professor Erik Jones, and it aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The RSCAS is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

Centre for a Digital Society

The Centre for a Digital Society (CDS) was created in 2022 and is directed by Prof. Pier Luigi Parcu. It analyses the challenges of digital transformation and its impact on markets and democracy. Within the EUI, the CDS is part of the Robert Schuman Centre for Advanced Studies. With its research, policy debates and executive training programmes, the CDS aims to advise policy makers on how to cope with the challenges that are generated by the digitalisation process. To do so, it adopts an inter-disciplinary approach, relying on in-house expertise in law, economics and political sciences, and by actively cooperating with computer scientists and engineers from partner institutions. For further information: https://digitalsociety.eui.eu/

Abstract

Data is often defined as the ‘oil’ of the 21st century economy: companies that successfully collect and process a large amount of data can provide more personalized services to their customers, develop new products, and reduce their production costs, thus becoming more competitive. Similarly, public institutions can provide more personalized services to citizens if they can access a large dataset. However, small firms and public institutions often cannot collect a sufficiently large amount of data on their own, and via data sharing small firms and public institutions can access larger and more diversified sets of data, thus boosting their efficiency. Despite its well-recognized benefits, several technical, regulatory and economics obstacles currently limit the degree of data sharing.

This paper first discusses the market failures that currently limit data ‘access’ and ‘re-use’ – which are jointly defined as ‘data sharing’. Secondly, the paper analyses the legislation recently adopted by the European Union (EU) to foster Business2Business (B2B), Government2Business (G2B) and Business2Government(B2G) data sharing, especially by comparing the terms of the compensation that is provided by the EU legislation. Finally, the paper analyses the meanings of Fair, Reasonable and Non-Discriminatory (FRAND) terms in the context of the licensing of Standard Essential Patents (SEPs) and access remedies in EU competition law, to draw some lessons on how the principle of FRAND, in the context of B2B data sharing, is interpreted.

Keywords

Data access; Data portability; Data Governance Act; Digital Markets Act; Data Act; FRAND; Standard Essential Patents; Antitrust access remedies

Contents

List of Figures

1. Introduction[1]

1.1 The data sharing paradox

Data is generally defined as the 'oil' of the 21st century economy:[2] companies that successfully collect and process a large amount of data (i.e., the, so-called, 'Big Data') manage to provide more personalized services to their customers and to reduce their production costs, thus becoming more competitive. During the past decade, online platforms have been proven to be successful in this regard, by collecting, combining, and extracting useful information from the personal data provided by their users. The advent of the Internet of Things (IoT) is expected to lead to an exponential growth in the number of 'data harvesting': sensors that are installed in different electronic devices and that collect an increasing amount of data, including non-personal data concerning the environment in which devices operate, as well as real-time diagnostic information about a device's functioning.[3] The larger amount of collected data is expected to improve the functioning of Artificial Intelligence (AI): data, in fact, is essential in order to train algorithms and thus to improve the quality of AI decision-making.[4]

The value of the EU data economy has steadily increased over the past decade.[5] However, the latter remains far less developed if compared to the US data market.[6] Countless studies have pointed out that improving access to data can foster a firm's competitiveness, and thus its economic growth.[7] The OECD, for instance, estimates that data sharing may lead to a GDP increase of between 0.1% and 1.5%, in the case of public sector data, and of between 1% and 2.5% when also including private sector data.[8] However, the same reports have also pointed out that only a limited number of firms currently 'share' their data with other companies. As President Von der Leyen noted, "…80% of the industrial data is collected and never used".[9] A similar conclusion was reached by the EU Commission in its 2020 Data Strategy.[10] In particular, data sharing is rather common among high tech firms, utilities, and providers of financial services, while public agencies, pharmaceutical companies and health care providers rarely grant third parties' access to their datasets.[11]

1 The author would like to thank Rupprecht Podszun, Inge Graef, Wolfgang Kerber, Klaudia Majcher, and Thomas Tombal for taking the time of reading and commenting previous versions of this working paper. Similarly, the author is thankful to Maria Way for having proof-read the paper before its publication. The author is fully responsible for every error and mistake in the paper.

2 Shannon Tellis, 'Data is the 21st Century's Oil, says Siemens CEO Joe Kaeser.' *The Economics Time*, 24.5.2018. The article is available at: <https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms?from=mdr> (last accessed 27.7.2022).

3 For an overview of the impact of IoT on business models and market dynamics, see McKinsey (2021), *Internet of Things: Catching up to an Accelerating Opportunity.* Report available at: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world> (last accessed 27.7.2022).

4 For an analysis of the impact of Big Data on firms' business models that rely on AI, see Ajay Agrawal, Joshua Gans and Avi Goldfarb. *Prediction Machines: The Simple Economics of Artificial Intelligence* (Harvard Business Review, 2018).

5 In a study published in 2022, the EU Commission estimated that, in 2014, the value of the EU data economy corresponded to 1.85% of the EU27's GDP. This value had increased to 2.4% in 2018, and it is expected to more than double by 2025.

European Commission, *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access right*, p.. 18. Published April 2022. The text of the study is available at:

<https://op.europa.eu/en/publication-detail/-/publication/dfb3a486-e6d4-11ec-a534-01aa75ed71a1> (last accessed 18.11.2022).

6 According to the 2020 EU Commission study, in 2019 the value of the EU data market was "approximately 2.5% smaller than that produced in the US."

European Commission, *The European Data Market Monitoring Tool.* Published on 6.7.2020, p. 9. The report is available at: <https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update> (last accessed 27.7.2022).

7 *Ibid.* p. 7.

8 OECD (2019), 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies.', p. 59-64. The text of the report is available at: <https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm> (last accessed 23.1.2023).

9 Ursula Von der Leyden, *Building the World We Want to Live in: A Union of Vitality in a World of Fragility. 2020 State of the Union speech*, delivered in Brussels on 16.9.2020. The speech is available at: <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655> (last accessed 27.7.2022).

10 in its 2020 Data Strategy, the EU Commission noticed that "…there is not enough data available for innovative re-use, including for the development of artificial intelligence."

European Commission Communication, A European Data Strategy. Published in Brussels on 19.02.2020. COM/2020/66 final, p. 6.

11 AIG (2016), 'The Data Sharing Economy: Quantifying Tradeoffs that Power New Business Models.' The report is available at: <https://www.familyoffice.com/knowledge-center/data-sharing-economy-quantifying-tradeoffs-power-new-business-models-part-3-series> (last accessed 23.1.2023).

The lack of interoperability among datasets, regulatory barriers, as well as security and data protection concerns, are the main obstacles to data sharing.[12] In addition, an incentive problem undermines data sharing: with the lack of a functioning market, firms cannot effectively assess the value of their dataset and[13], as a consequence, either firms decide to opt for an open access approach (i.e., requesting no compensation) or, more often, decide not to share their dataset.[14] As pointed out by the EU Commission, data sharing should be compensated: without compensation, in fact, the party collecting the data would not have any incentive to share its dataset with third parties.[15] In a nutshell, we are witnessing a sort of 'data sharing paradox': on the one hand, data is acquiring an increasing value in the 21st century economy; access to data becomes essential for every firm operating in the digital economy. On the other hand, due to several obstacles, firms are reluctant to share the collected data; they prefer to 'seal' the data, rather than concluding a sharing agreement with a third party.[16] The data sharing paradox does not only affect business2business (B2B) transactions: the barriers mentioned above also affect the sharing of data between public agencies and the private sector, and vice versa (i.e., G2B and B2G data sharing).

In order to tackle the data sharing paradox, during the recent years, the European Union has developed a new legal framework. As explained by the EU Commission in its 2020 Data Strategy, the new regulatory framework includes two 'layers':[17] on the one hand, the EU is supporting the creation of Common European Data Spaces in strategic sectors, in order to overcome the technical, privacy and security barriers that currently undermine data sharing in specific industries.[18] Secondly, the EU Commission has put forward a number of cross-sector legislative proposals to establish a common EU regulatory framework on data sharing. In 2020, the European Commission proposed a Data Governance Act (DGA),[19] aiming at stimulating government2business (G2B) data sharing. The DGA, recently approved by the Council and the European Parliament, complements the 2019 Open Data Directive (ODD).[20] Secondly, in February 2022, the Commission proposed a Data Act, which aimed to stimulate business2business (B2B) data sharing, as well as to mandate data sharing from the private to the public sector (i.e., B2G data sharing) in case of a public emergency.[21] Thirdly,

12 Richard Feasy and Alexandre De Streel (2020), 'Data Sharing for Digital Markets' Contextability. Towards a Governance Framework.' CERRE Report, published in September 2020, p.. 15. The report is available at: <https://cerre.eu/publications/data-sharing-digital-markets-competition-governance> (last accessed 27.7.2022).

13 Deloitte, *Study on Emerging Issues of Data Ownership, Interoperability, Re-usability and Access to Data and Liability. Study on behalf of the European Commission*, published in 2018, p.. 56. The study is available at: <https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en> (last accessed 27.7.2022).

14 According to the 2018 Deloitte study, only 15% of the firms that joined the study actively engaged in data sharing, and they usually opt for the open data regime.

Ibid, p. 57.

15 According to the EU Commission, "the term 'sharing' should not be understood as meaning 'for free'."

European Commission, Study on data sharing between companies in Europe. Published in 2018, p.. VIII. The text of the study is available at: <https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en> (last accessed 18.11.2022).

16 Alberto Alemanno (2018), 'Big Data for Good: Unlocking Privately Held Data to the Benefit of the Many.' 9 *European Journal of Risk Regulation:* 185.

17 *Supra,* EU Data Strategy, p. 12.

18 After having been announced in the 2020 Data Strategy, the European Commission provided further details about the Common European Data Spaces in the Staff Working Document published in February 2022. The European Commission plans to establish, in the coming years, Common Data Spaces in relation to health care, industrial manufacturing, agriculture, finance, mobility, the Green Deal, energy, public administration and skills. The objective of each Data Space is to establish a single market for data, thus favouring data sharing among the firms operating in a specific industry. For each Data Space, the European Commission will put forward common interoperability standards, sectoral data governance rules (i.e., model contracts, licenses, access rights), while the EU budget will finance the development of a common IT infrastructure for each Data Space.

European Commission Staff Working Document on Common European Data Spaces. Published in Brussels on 23.2.2022, SWD(2022)45 final. The document is available at: <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces> (last accessed 18.11.2022).

For further information concerning the development of the Common European Data Spaces initiative see <http://dataspaces.info/common-european-data-spaces/> (last accessed 18.11.2022).

19 Regulation 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). OJ L-152/1, 3.6.2022.

20 Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019, on open data and the re-use of public sector information. OJ L-172/56, 26.6.2019.

21 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data* (Data Act). COM/2022/68 final. Published in Brussels on 23.2.2022.

the Digital Market Act (DMA),[22] which was recently adopted by the Council and the European Parliament, includes a number of specific data sharing obligations, mandating digital gatekeepers to share their data with competitors under certain circumstances. The DMA complements sector-specific rules, which mandate data sharing in specific industries, such as in the chemical,[23] banking,[24] automotive,[25] electricity,[26] telecom[27] and postal sector.[28] Finally, the right to data portability may also be considered part of the EU data sharing legal framework: Art. 20 of the General Data Protection Regulation (GDPR), in fact, empowers the data subject to request the data controller to transfer his/her personal data to a third party, which results in a B2B data sharing transaction.[29]

The new EU legal framework, therefore, covers both B2B, G2B and B2G data sharing. The framework aims to stimulate data sharing by introducing a common EU regulatory framework (i.e., increasing legal certainty), rather than imposing a sharing obligation.[30] Mandated data sharing is introduced only in specific circumstances, in which the EU legislator identifies either a specific market failure or a reason that is of public interest (e.g., the B2G data sharing obligation in the case of a public emergency), which justify a direct intervention in market dynamics. Mandated data sharing is thus the exception, rather than the general rule, within the new EU regulatory framework.

1.2 Objectives of the paper

The paper aims to analyse the emerging EU regulatory framework on data sharing, focusing on the provisions concerning the conditions for sharing and the remuneration level. The legislations mentioned in the previous section diverge from this point of view, opting either for an open access regime (i.e., zero remuneration for the data holder), or following a Fair and Reasonable and Non-Discriminatory (FRAND) compensation approach. The paper aims to compare the different systems of compensation and sharing conditions that are emerging in the new EU legislative framework, thus assessing the consistency of such a framework. Secondly, the paper investigates the meaning of FRAND in the context of data sharing, looking at the lessons learnt from EU competition law remedies and at the licensing conditions for Standard Essential Patents (SEPs), in which FRAND is a rather well-established principle.

22 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, amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L-265/1, 12.10.2022.

23 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December, 2006, concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94, as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC. OJ L-396/1, 30.12.2006.

24 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 (PSD2 Directive). OJ L-337/35, 23.12.2015. Art. 36.

25 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018, on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009, and repealing Directive 2007/46/EC. *OJ L-151/1, 14.6.2018. Art. 61.*

26 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019, on common rules for the internal market for electricity and amending Directive 2012/27/EU. OJ L-158/125, 14.6.2019. Art. 23.

27 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018, establishing the European Electronic Communications Code (EECC). *OJ L-321/36, 17.12.2018. Art. 112.*

28 Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008, amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services. OJ L-52/3, 27.2.2008. Art. 11a.

29 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons about the processing of personal data, and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR). OJ L-119/1, 4.5.2016. Art. 20.

30 "The European Commission's general strategic focus has been on encouraging and facilitating voluntary data sharing, rather than on introducing any obligation to share data."

Supra, European Commission Study on Model Contract Terms in Data Sharing, p..7.

A number of authors have extensively commented on the new EU legislative framework, and,in particular, focusing on the DMA,[31] the Data Act proposal,[32] as well as on the GDPR provisions for data access and portability.[33] Secondly, a strand of literature has discussed the technical and regulatory barriers that undermine data sharing,[34] as well as the potential conflict with data protection rules.[35] Thirdly, a number of authors have discussed the topic of data governance,[36] mostly by looking at the role of data intermediaries.[37] Finally, some scholars have debated whether, and to what extent, data may be the subject of a new *sui generis* intellectual property right.[38] By contrast, only few authors have looked at the issues relating to the compensation and sharing conditions.[39] The paper thus aims to fill a gap in the literature, in order to better understand whether, and to what extent, the new EU legislative framework is 'fit for the purpose' of stimulating data sharing.

31 See, for instance:
- Pinar Akman (2022), 'Regulating competition in digital platform markets: a critical assessment of the framework and approach of the EU Digital.' 47(1) *European Law Review:* 85-114.
- Pierre Larouche and Alexandre De Streel (2021), 'The European Digital Markets Act: A Revolution Grounded on Traditions' 12(7) *Journal of Competition Law and Practice:* 542-560.
- Marco Botta (2021), 'Sector Regulation of Digital Platforms in Europe: Uno, Nessuno e Centomila.' 12(7) *Journal of Competition Law and Practice:* 500-512.

32 See, for instance:
- Inge Graef, Martin Husovec (2022), 'Seven Things to Improve in the Data Act.' Published on SSRN on 7.3.2022. The paper is available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793> (last accessed 27.7.2022).
- Wolfgang Kerber (2022), 'Governance of IoT Data: Why the EU Data Act Will Not Fulfill its Objectives.' Published on SSRN on 27.7.2022. The paper is available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436> (last accessed 27.7.2022).
- Rupprecht Rodszun and Philipp Offergeld (2022), 'The EU Data Act and the Access to Secondary Markets.' The paper is available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4256882> (last accessed 27.1.2023).

33 See, for instance:
- Jan Krämer, Pierre Senellart, Alexandre De Streel (2020), 'Making Data Portability More Effective for the Digital Economy.' CERRE report published in June 2020. The report is available at:
https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/ (last accessed 16.7.2022).
- Inge Graef, Martin Husovec, Nadezhda Purtova (2018), 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law.' Vol 19, Issue 6, *German Law Journal:* 1359-1398.
- Orla Lynskey (2017), 'Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability' Vol. 42, Issue 6, *European Law Review:* 793-814.

34 See, for instance:
- Marc Bourreau, Jan Krämer, Miriam Buiten (2022), 'Interoperability in Digital Markets.' CERRE report published in March 2022. The report is available at: <https://cerre.eu/publications/interoperability-in-digital-markets/> (last accessed 27.7.2022).
- Michal Gal and Daniel Rubinfeld (2019), 'Data Standardization.' 94 *New York University Law Review:* 737-769.

35 See, for instance, Barbara Engels (2016), 'Data Portability among Online Platforms.' 5(2) *Internet Policy Review:* 1-17.

36 See, for instance:
- Inge Graef and Jens Prüfer (2021), 'Governance of Data Sharing: a Law and Economics Proposal.' 50(9) *Research Policy:* 1-14.
- Nicolo Zingales, 'Data collaboratives, competition law and the governance of EU data spaces.' In Ioannis Kokkoris, *Research Handbook on the Law and Economics of Competition Enforcement* (Edward Elgar Publishing, Cheltenham, 2022). Chapter 1, pp. 8-49.

37 See, for instance, UK Centre for Data Ethics and Innovation, 'Unlocking the Value of Data: Exploring the Role of Data Intermediaries.' Report published in July 2021, available at: <https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries> (last accessed 27.7.2022).

38 Zech was the first author to propose a new *sui generis* IP right for data, which are considered to be a new tradable commodity. According to Drexl, on the other hand, data should be subject to an access regime, rather than to a new intellectual property right, which would limit data sharing.
Herbert Zech, 'Data as tradeable commodity' in Alberto de Franceschi (ed.), *European Contract Law and the Digital Single Market* (Insentia, 2016), pp. 51-80.
Josef Drexl (2016), 'Designing Competitive Markets for Industrial Data – between Propertisation and Access.' Max Planck Institute for Innovation and Competition Research Paper No. 16-13.

39 See, in particular:
- Diane Coyle, Stephanie Diepeveen, Julia Wdowin (2020), 'The Value of Data. Policy Implications.' Report published February 2020 by the Bennett Institute of Public Policy. The report is available at: <https://www.bennettinstitute.cam.ac.uk/publications/value-data-policy-implications/> (last accessed 27.7.2022).
- Peter Picht and Heiko Richter (2021), 'The Proposed EU Digital Services Regulation 2020: Data Desiderata.' Max Planck Institute for Innovation and Competition Research paper No. 21-21. The paper is available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3925359> (last accessed 27.7.2022).
- Erik Habich (2022), 'FRAND Access to Data: Perspectives from the FRAND Licensing of Standard-Essential Patents for the Data Act Proposal and the Digital Markets Act. 53 IIC: 1343-1373.
- Peter Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law.' Max Planck Institute for Innovation and Competition Research Paper No 22-12. The working paper is available at: <https://www.ip.mpg.de/en/publications/details/caught-in-the-acts-framing-mandatory-data-access-transactions-under-the-data-act-further-eu-digital-regulation-acts-and-competition-law.html> (last accessed 23.1.2023).
- Giorgio Monti, Thomas Tombal, Inge Graef (2022), 'Study for Developing Criteria for Assessing "Reasonable Compensation" in the Case of Statury Data Access Right." Study carried out on behalf of DG Justice and Consumers of the European Commission. The study is available at: <https://op.europa.eu/en/publication-detail/-/publication/599678d8-79d2-11ed-9887-01aa75ed71a1/language-en/format-PDF/source-277469567> (last access 20.3.2023).

The paper is structured as follows: Section 2 sets out the context, discussing the meanings of 'data' and 'data sharing' from a legal point of view, analysing the business models and the economic actors involved in such a process, as well as the economic incentives and the obstacles to data sharing. Section 3 analyses different typologies of data sharing in the context the new EU regulatory framework, focusing on the issue of compensation and sharing conditions. Section 4 compares the concept of FRAND in the context of SEP licensing and in EU competition law remedies, to elaborate useful lessons to apply in the context of B2B data sharing. Finally, Section 5 concludes.

The paper opts for a 'holistic approach' to data sharing. In particular, the paper deliberately includes the GDPR within the EU regulatory framework on data sharing. Although the expression 'data portability' usually refers to a data subject's right under Art. 20 GDPR, the Data Act proposal includes a similar users' right in relation to the non-personal data generated by a product's use.[40] In light of the holistic approach followed in the paper, the term 'data portability' deliberately covers the sharing of both personal and non-personal data. Secondly, from a terminological perspective, the paper relies on the expression 'data sharing'.

Secondly, as noted by Richter and Slowinski, 'data sharing' is a broad expression, which covers two scenarios: [41] the data holder may grant a third party 'access' to its database. Access may take place either *in situ* or remotely. Alternatively, the data holder may provide to a third party the right to 're-use' certain data for a different purpose than the initial objective of processing by the data holder. As further discussed in Section 2, these two methods are common when private firms exchange data (B2B), but also when public and private agencies interact (i.e., G2B and B2G data sharing). In view of its 'holistic approach', the current papers generally use the expression 'data sharing' rarely when covering both 'access' and data 're-use'.

In terms of its scope, this paper discusses the emerging EU cross-sectoral regulatory framework on data sharing, while the Common European Data Spaces remain beyond the scope of the paper. Secondly, the paper discusses general market incentives and obstacles to data sharing, especially in terms of compensation conditions, rather than the technical, privacy and security barriers that undermine the sharing process. The latter barriers, in fact, will be mostly addressed via *ad hoc* solutions in the context of Common European Data Spaces, rather than within the EU cross-sector regulatory framework that is at the core of the paper. Finally, the paper focuses on B2B, G2B and B2G data sharing, since these last typologies are at the core of the EU regulatory framework on data sharing. By contrast, the paper does not analyse other modalities of data sharing, such as G2G data sharing. Similarly, the paper does not discuss the conditions under which public and private firms may collect data from individuals under Art. 6 GDPR, as well as the conditions under which individuals may access their data under Art. 15 GDPR.

40 *Supra,* Art. 6 proposed Data Act.

41 Heiko Richter, Peter Slowinski (2019), 'The Data Sharing Economy: on the Emergence of New Intermediaries.' 50 *IIC:* 4-29. At 8.

The Preamble of the proposed Data Act points out that "this Regulation complements the right provided under Article 20 of the Regulation (EU) 2016/679" – i.e., the right to data portability under the GDPR.

Supra, Data Act proposal, preamble, para. 31.

2. Data sharing

2.1. Some terminology

2.1.a. The legal definition of 'data'

The proposed Data Act defines 'data' as "… any digital representation of acts, facts or information and any compilation…, including in the form of sound, visual and audio-visual recording."[42] The same definition can also be found in the DMA[43] and in the DGA,[44] thus representing a common feature of the emerging EU legal framework on data sharing.

The EU definition of 'data' is rather broad: it covers every type of information that can be represented in a 'digital' format – i.e., information that can be translated into a 'binary' digital code.[45] Secondly, the definition includes individual data items, as well as data 'compilations' (i.e., datasets). While a database refers to a collection of data that is: "…arranged in a systematic and methodological way and individually accessible….",[46] a dataset does not need to meet any specific innovation/ organizational threshold.

From a legal perspective, the expression 'data' covers two distinct categories, while the expression 'personal data' refers to all of the information that would allow for the identification of a natural person (i.e., the data subject),[47] 'non-personal data' is a catch-all category, which generally refers to information that does not allow such identification.[48] Such a distinction is important in the context of the GDPR: data protection rules, which are, in fact, applicable only to information, either stored in a digital or in a non-digital format, which allows the identification of an individual (e.g., name, date of birth, address, gender…).[49] Personal data may be processed only when there is a lawful legal basis, such as is the case when the data subject provides his/her consent to the processing of the data, or in the case that the processing is needed to perform a contract that has previously been concluded by the data subject, or to comply with a legal obligation.[50] By contrast, no specific legal basis is needed to collect and process machine-generated data, as long as the latter does not include personal data.[51]

The distinction between personal and non-personal data is not always straightforward. Personal data, in fact, may be freely processed by the data holder if it is aggregated and 'anonymized' – i.e., no specific natural person can be identified during the processing of the data.[52] Nevertheless, even anonymized data may be subject to data protection rules if, following data analytics, individuals can be re-identified.[53] Due to the limits of the anonymization process, Tombal has concluded that

42 *Supra,* Art. 2(1) Proposed Data Act.
43 *Supra,* Art. 2(24) DMA.
44 *Supra,* Art. 2(1) DGA.
45 According to Encyclopaedia Britannica, the 'binary code' is the code used by computers; it is based on a binary number system in which there are only two possible states, off and on, usually symbolized by 0 and 1.
<https://www.britannica.com/technology/binary-code> (last accessed 8.8.2022).
46 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996, on the legal protection of databases. OJ L-77/20, 27.3.1996. Art. 1(2).
47 *Supra,* Art. 4(1) GDPR.
48 The EU legal framework does not provide for a separate definition of non-personal data. Art. 3(1) Reg. 2018/1807, which establishes an EU legal framework for the free flow of non-personal data, defines it as "data other than personal data, as defined in point (1) of Article 4 of Regulation (EU) 2016/679." Non-personal data is thus a catch-all category, which includes any form of data that does not fall within the GDPR's scope of application.
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. OJ L-303/59, 28.11.2018.
49 *Supra,* Art. 5 GDPR.
50 *Supra,* Art. 6 GDPR.
51 "The principles of data protection should therefore not apply to anonymous information, namely, information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."
Supra, para. 26, preamble GDPR.
52 *Supra,* Art. 4(5) and Art. 25 GDPR.
53 *Supra,* Tombal (2022), p. 17.

the classic distinction between personal and non-personal data has a rather "porous boundary".[54] Tombal thus proposes a new data typology, based on the way in which the data has been generated/acquired, rather than on the classic distinction between personal and non-personal data.[55] According to Tombal, data may be either 'actively provided' by an individual to the data controller, or 'observed' by the controller; following data mining, the controller/holder may also 'infer/derive' some additional data. Finally, both personal and non-personal data may be 'acquired' – i.e., via data sharing. As mentioned in the introduction, the current paper follows a similar holistic approach, analysing the data sharing of both personal and non-personal data.

2.1.b. The legal definition of 'data sharing'

According to the Data Governance Act, data sharing means: "…the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge."[56]

The definition of data sharing provided by the DGA is broad; it is a 'label' that covers rather different types of transactions and actors.[57] Firstly, by referring both to the 'data subject' and to the 'data holder', the definition clearly covers both personal and non-personal data. As is further explained in the following pages, data sharing may take place between different actors, including private parties (i.e., B2B), as well as public and private actors (i.e., G2B and B2G).

It is worth noticing that the DGA refers to 'sharing', rather than to data 'transfer'. Within the EU legal framework, in fact, data 'transfer' generally refers to the possibility of transferring personal and non-personal data outside of the EU.[58] Secondly, in the lack of an exclusive property right, the data holder does not 'transfer' any ownership to the recipient; rather, the holder provides 'access' to its dataset, and thus keeps the right to continue using the collected data.[59] Alternatively, the data holder may grant to the recipient the right to 're-use' the dataset for a different purpose.[60] Data re-use is particularly important in stimulating innovation,[61] as, while the original data holder, in fact, would not further process the collected data, the recipient could use the dataset to develop a new product/service. Access and re-use do not necessarily have to be 'unlimited': the parties could mutually agree on sharing and re-use limitations in the context of the contract. Nevertheless, it is important to bear in mind that neither access nor re-use implies a transfer of the data ownership.

It is also worth pointing out that the word 'sharing' does not imply a lack of compensation (i.e., according to the DGA, data sharing may be "subject to a fee or free of charge").[62] Compensation is generally considered important, in order to generate sufficient incentives for the data holder to further collect data and improve the quality of its dataset.[63] As further discussed in Section 3, firms and public agencies may be forced to share data 'for free' in cases of mandated data access; the latter, however, represent an exception within the EU legal framework on data sharing, rather than representing the general rule. Secondly, compensation does not necessarily have to be monetary

54 Thomas Tombal, "Imposing Data Sharing among Private Actors." (Kluwer Law International, 2022). Chapter 1.2.
55 *Ibid,* Chapter 1.3, Figure 1.1.
56 *Supra,* Art. 2(10) DGA.
57 Bertin Martnes et al (2020), "Business-to-Business Data Sharing: an Economic and Legal Analysis." JRC Digital Economy Working Paper 2020-05. P. 14.
58 According to the GDPR, personal data may be transferred from the EU to a third country only if the EU Commission has previously issued a decision, confirming that the third country ensures an adequate degree of data protection. Similarly, according to the proposed Data Act, providers of data processing services may transfer non-personal data only to third countries with whom the EU has previously concluded a mutual assistance treaty.
Supra, Art. 44-50 GDPR.
Supra, Art. 27 proposed Data Act.
59 European Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 25.4.2018. COM(2018)232 final, p.. 9.
60 *Supra,* European Commission study on data sharing between companies in Europe, p. 2.
61 *Supra,* European Commission study on data sharing between companies in Europe, p. 2.
62 *Supra,* European Commission study on data sharing between companies in Europe, p. VIII.
63 European Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Building a European Data Economy.* Published in Brussels on 10.1.2017. COM(2017)9 final, p..

compensation: in B2B data sharing, for instance, parties may decide to mutually grant access to their datasets (i.e., data polling).

Finally, it is worth noting that, as a general rule, data sharing may be arranged according to a contract, concluded by the data holder and the recipient (i.e., according to the DGA definition, "on a voluntary basis"), and eventually via an intermediary.[64] In certain situations, however, data sharing may be 'regulated' by law (i.e., on the basis of "Union or national law").[65] Firstly, data sharing may be required by law in order to solve a number of market failures, such as information asymmetries,[66] and excessive market power.[67] Secondly, data sharing may be mandated for reasons of public interest: the proposed Data Act, for instance, requires the data holder to share data with a public authority in the case of there being a "public emergency".[68]

To sum up, the EU legal framework includes broad and inclusive definitions of 'data' and 'data sharing'. Both expressions cover both personal data, which is subject to the GDPR's protection, as well as non-personal data. In principle, every type of data may be shared by the data holder with a third party; even personal data may be shared, provided that either one legal basis under Art. 6 GDPR is fulfilled (e.g., the data subject has provided his/her consent), or the data has been fully anonymized. As clarified by the DGA preamble, in fact, in the case that there is conflict between the EU data sharing rules and the GDPR, the latter "should prevail".[69]

2.2. Data sharing from a practical point of view

From a technical point of view, data sharing may take place in accordance with different modalities, which vary depending on the number of repeated interactions between the data supplier and the recipient. On the one hand, we may have a situation in which the recipient receives a 'copy' of the entire/part of the holder's dataset.[70] The copy can be provided in different formats (e.g., printed document, DVD …). Independently of the format selected, this type of data sharing is 'static' – i.e., the copy can hardly be updated after the first sharing, unless a further copy of the dataset is shared between the parties. Secondly, the recipient has full control over the shared data.

Alternatively, the recipient can access 'synthetic' data representation.[71] The latter is a type of description of the raw data that is included in the dataset. For instance, rather than listing the name, surname, address… of the people included in the database, a synthetic data representation could offer a visual description of the towns in which the data subjects live, without providing any information concerning their addresses. Synthetic data representation allows the anonymization of the personal data included in the dataset; such representations are usually automatically generated by an algorithm in the context of the anonymization process.

Thirdly, data may also be shared in 'real-time':[72] the data holder provides, usually via cloud computing, access to the dataset by the recipient. Real-time access is convenient for both parties: on the one hand, the recipient receives up-to-date data; on the other hand, the holder keeps constant control over the shared data (e.g., the holder can limit data sharing to certain categories of data, such

64 *Supra,* Art. 2(10) DGA.
65 *Supra,* Art. 2(10) DGA.
66 According to the 2019 Electricity Directive, for instance, Transmission System Operators (TSO) should provide access to "metering and consumption data" for final consumers, as well as to other electricity suppliers. Via the shared data, in fact, third suppliers may make more targeted offers to the consumers, thus incentivizing them to switch supplier, thus fostering market competition.
Supra, Art. 23 Directive 2019/944.
67 In the sector relating to digital advertising, for instance, online platforms often act as gatekeepers between publishers and advertisers. Under Art. 6(8) DMA, digital gatekeepers that operate in the sector shall provide to publishers and advertisers "aggregated and non-aggregated data" about advertisements, so that publishers and advertisers can verify the effectiveness of an advertising campaign.
Supra, Art. 6(8) DMA.
68 *Supra,* Art. 14-15 Data Act proposal.
69 *Supra,* para. 4, preamble DGA.
70 *Supra,* Tombal (2022), para. 105.
71 Ibid.
72 Ibid.

as non-personal data).

Finally, data may also be shared via a 'question and answer model',[73] as with real-time access, the recipient obtains remote access to the dataset, benefiting from its continuous updating. Nevertheless, the access is not unlimited: the recipient must ask the holder to allow access to a type of data. Clearly, a question-and-answer model allows the data holder to keep a stronger degree of control over the shared data.

2.3. Data sharing business models

Data sharing may take place in accordance with different 'models', which are influenced by a number of factors, such as the type of data to be shared (i.e., personal v. non-personal data), the actors involved (i.e., B2B, G2B, B2G data sharing), the industry specificities, as well as by the business model that has been selected by the data holder. There are thus a multitude of data sharing models, which are difficult to categorize, and the number of business models is increasing with the development of data sharing.

2.3.a. B2B data sharing

In the context of B2B data sharing, a bilateral agreement between companies to grant data access/re-use in exchange for monetary compensation is quite rare, in practice.[74] When companies want to share non-personal data, they often establish '**data platforms'**, which allow participants to exchange their industrial data within a secure environment.[75] Participants, in fact, can agree on common Application Programming Interfaces (APIs), which facilitate data sharing from a technical point of view. In other words, data platforms remove some of the barriers to data sharing, and this is further discussed in the pages that follow, e.g., security and interoperability considerations. In terms of compensation, platform participants are remunerated by having access to a common/larger data pool, rather than by receiving monetary compensation for every transaction.[76] Skywise is an example of a data platform. It was established among Airbus and the airlines which have purchased Airbus airplanes for their commercial fleets.[77] The airlines participating in the the Skywise programme freely provides to Airbus real-time diagnostic data about their airplanes. This data allows Airbus to test the functioning of its airplanes in different scenarios, thus allowing Airbus to improve the technical qualities of its airplanes in the long term. In the short term, however, Airbus monitors the 'health' of the vehicles and can thus provide information about the predictive maintenance of the airplanes; via real-time diagnostics, the airlines can reduce the risk of accidents, as well as the airplanes' maintenance costs. Finally, it is worth noting that when data platforms are concluded between competitors, they represent a horizontal cooperation agreement, which may be subject to competition law scrutiny.[78]

An alternative model of B2B data sharing is the so-called '**marketplace'**. Unlike a data platform, a marketplace is open to a potentially unlimited number of data holders and recipients. The marketplace works as an intermediary between the parties, acting as the matchmaker between the potential data suppliers and the buyers, thus providing a framework in which to allow the transaction to take place and, *ex-post,* certifying that a data sharing transaction has taken place. [79] Snowflakes is an example of a data marketplace: it provides access to several types of datasets that are offered by different providers. Snowflakes categorizes the datasets under different typologies (e.g., financial,

73 Ibid.

74 *Supra,* European Commission, *Study on model contract terms and fairness control in data sharing*, p. 56.

75 *Supra,* 2018 European Commission Staff Working Paper on Common European Data Space, Section 3.3.

76 *Supra,* Tombal (2022), para. 110.

77 <https://aircraft.airbus.com/en/services/enhance/skywise> (last accessed 22.11.2022).

78 The revised Horizontal Cooperation Guidelines, published by the EU Commission in March 2022, point out that participants in a data pool may only have access to the data provided, as well as to the aggregated data generated by the pool. In other words, the data pool should not become a mechanism with which to allow the exchange of sensitive business information among competitors.
European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements. Brussels, 1.3.2022, C(2022) 1159 final. Para. 440.

79 *Supra,* 2018 European Commission Staff Working Paper on Common European Data Space, Section 3.3.

government, healthcare, travel, weather…).[80] The buyer selects which dataset to download; after the first downloading, the dataset is automatically updated by the provider. In terms of remuneration, Snowflakes follows a standard subscription fee, while other marketplaces may opt for an *ad hoc* fee for the downloading of each dataset, a fee which has previously been defined by the data holder.[81]

Marketplaces simply facilitate the data sharing process, but they do not always guarantee the interoperability of the acquired data with the buyer's dataset. An alternative solution is represented by the '**technical enablers'** – i.e., the intermediaries, which provide a number of services to both the data supplier and the recipient, in addition to facilitating the transaction.[82] Unlike a simple marketplace, the technical enabler will also design APIs to facilitate the data sharing process and to provide anonymization services for the personal data, in order to solve in advance any data protection concerns. Nallian is a good example of a technical enabler.[83] This company has developed a cloud-based platform that enables real-time data sharing in the context of air cargo transportation. Nallian allows air cargo firms, ground handlers, freight forwarders, trucking companies, carriers, shippers, and the airport administration, to have access to the real-time data relating to specific cargo. By facilitating the exchange of data between different logistics firms, placed on different levels of the supply chain, Nallian reduces the delivery time of air cargo. Nallian, and other technical enablers, mostly work based on a subscription fee, which is paid by the firms that would like to have access to the data sharing platform provided by Nallian.

Data platforms, marketplaces and technical enablers are the three main business models in B2B data sharing. However, these models are not exhaustive; as mentioned above, the data sharing models are constantly evolving. Overall, it is worth noting that bilateral B2B data sharing rarely takes places in practice. Similarly, monetary compensation that is based on a fee paid for each transaction is also quite uncommon; firms would rather provide their data in exchange for other data, or by paying a standard subscription fee. Even when data is shared 'for free', the data supplier is expected to receive a service from the data recipient (see, for example, the diagnostic data provided by Airbus to the airline companies who are members of the Skywise programme). The different models of compensation are an important aspect of assessing the EU legal framework on data sharing, as is further discussed in Section 3.

2.3.b. G2B and B2G data sharing models

Government2business (G2B) and Business2government (B2G) data sharing often follow the same B2B sharing modalities. Public institutions, in fact, often establish platforms, marketplaces and technical enablers to provide data to private operators. In 2013, for instance, Hitachi, a leading Japanese IT firm, won the public tender organized by the municipality of Copenhagen, which aimed to establish a platform on which to facilitate G2B data sharing.[84] Via this project, Copenhagen's city administration aimed to establish a common platform on which to share local mobility data with apps' developers and the providers of mobility and advertising services.[85] Amongst others, the data sharing aimed to reduce traffic congestion in the city. Similarly, in 2018, the French government established a *Centre d'Accès Sécurisé aux Données* (CASD, Centre for Secure Data Access) – i.e., a common data platform on which to share the datasets generated by different public authorities in France.[86] Via a centralized sharng platform, CADS ensures compliance with safety and data protection rules. In order to access CASD datasets, the potential receiver has to pay a monthly fee, which is influenced by the number of users that will have access to the data platform and the number of datasets to

80 <https://www.snowflake.com/guides/what-data-marketplace> (last accessed 22.11.2022).
81 <https://www.forbes.com/sites/forbestechcouncil/2021/05/12/the-ins-and-outs-of-a-data-marketplace/?sh=4d8ed6da19ea> (last accessed 22.11.2022).
82 *Supra,* 2018 European Commission Staff Working Paper on Common European Data Space, Section 3.3.
83 <https://nallian.com/about-us> (last accessed 22.11.2022).
84 <https://www.copcap.com/newstmp/hitachi-builds-big-data-platform-for-copenhagen> (last accessed 28.11.2022).
85 <https://cphsolutionslab.dk/media/site/1837671186-1601734920/city-data-exchange-cde-lessons-learned-from-a-public-private-data-collaboration.pdf> (last accessed 28.11.2022).
86 <https://www.casd.eu/en/le-centre-dacces-securise-aux-donnees-casd/gouvernance-et-missions/> (last accessed 28.11.2022).

which the users will gain access.[87]

While Copenhagen and CASD established centralized platforms to share public data with a plurality of business actors, several public institutions have established cooperation platforms, on which they actively transfer data to business operators in exchange for other data. Waze Connected Citizens program is a good example of this sharing modality.[88] Waze is a well-known navigation app; unlike Google and Apple maps, Waze users can share real-time information about traffic jams and road closures; the algorithm collects and processes the data, and it shares up-to-date road information with Waze users. In the context of the Connected Citizens program, Waze has concluded data sharing agreements with the municipal administrations of several cities around the world. The cities share with Waze real-time information about traffic congestion and road closures, and, at the same time, Waze also shares the data collected by its users with the local police and municipal authorities. Waze Connected Citizen program is a case of B2G and G2B data sharing, in which both parties exchange similar types of data to in order to solve traffic congestion issues.

Finally, a number of public authorities have facilitated G2B data sharing by opting for a technical enabler, rather than a data platform or a marketplace. By establishing Findata, for instance, the government of Finland introduced a system to facilitate the data sharing of the health care data of Finnish citizens, to foster medical research.[89] Findata not only shares the data, but it checks that these data have been aggregated and anonymized before being shared, so as to comply with data protection rules.

In addition to platforms, marketplaces and technical enablers, G2B and B2G are characterized by specific data sharing typologies, which are not present in the B2B scenario. Contrary to the B2B scenario, in fact, data sharing between public and private institutions does not necessarily take place for a 'remuneration'; there may be non-economic goals at the origin of the sharing process, such as fostering research, or reducing traffic and energy consumption[90]. In addition, the data may be shared for 're-use', rather than being specifically collected and processed to be shared. A few public institutions have opted for an '**open data model'** to foster data re-use. Data.Gov, is an initiative of the US government to share, via an integrated open platform, different datasets that are generated by US federal agencies.[91] In Europe, statistical offices and weather forecasting agencies have engaged in open data sharing in relation to the different datasets. However, only a few of the EU Member States have so far followed the example of Data.Gov and established centralized agencies that oversee administering an open data policy.

An alternative model that is emerging in the context of G2B data sharing is the so-called '**civic data sharing/data altruism'**'.[92] Individuals are increasingly aware of the relevance of their personal data in achieving different objectives that are of public interest; individuals are increasingly aware that they can pull their personal data together, and that they can share the aggregated data with third parties in order to achieve objectives that are of general interest.[93] Midata is a data cooperative that is funded by ETH Zurich and a group of public universities in Switzerland.[94] The Midata project aims to collect health care data via an app that can be installed on smart watches and mobile phones. Individuals who download the app agree to provide a number of items of personal information to Midata, together with real-time health data (e.g., blood pressure, body temperature, heart rate). The platform shares the aggregated data that is provided by individuals with pharmaceutical companies and other actors who are involved in research on new medicines and medical therapies. Individuals

87 <https://www.casd.eu/en/tarifs-2/> (last accessed 28.11.2022).

88 <https://wazeopedia.waze.com/wiki/UAE/Connected_Citizens_Program/> (last accessed 29.11.2022).

89 <https://findata.fi/en/> (last accessed 28.11.2022).

90 For an overview of the benefits of an open data approach, see: European Commission, Creating Value through Open Data. Report published in 2015. The study is available at: <https://data.europa.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf> (last accessed 28.11.2022).

91 <https://data.gov/> (last accessed 28.11.2022).

92 *Supra, Supra,* 2018 European Commission Staff Working Paper on Common European Data Space, Section 4.

93 Marina Micheli and others (2020), 'Emerging Models of Data Governance in the Era of Datafication.' July-December *Big Data and Society:* 1-15.

94 <https://www.midata.coop/it/homepage/> (last accessed 28.11.2022).

who join the project always have full control of their data which, in any case, are shared in an anonymous manner with third parties. Midata applies an open data policy – i.e., the data are shared, free of charge, with third parties. Midata acts as a 'trusted intermediary' between individuals and data recipients; a similar model may exist in B2G data sharing, whenever a third-party acts as an intermediary between the business data provider and the public data recipient.

Data may also represent the '**prize' / 'award'**, which is shared by public and private data holders with qualified recipients.[95] The prize/award model is common in the research area, and it can take place in the context of both G2B and B2G data sharing: a private firm, for instance, can share a dataset with a public university, in order to carry out specific research. Alternatively, a public institution can share its dataset with a firm that is committed to using it for specific research. In both cases, we are talking about the re-use of an existing dataset, shared via an open access approach, in order to achieve an objective of general interest. An example of B2G data prize/award is represented by the Mastercard Centre for Inclusive Growth.[96] During the past decade, Mastercard has shared a large amount of data concerning financial transactions, which has been collected from around the world, with government agencies and no profit organizations, to foster access to credit, and thus to fostering economic growth in under-developed regions of the world.

Similarly to the data prize/award model, firms may also share their data with public entities in the context of public emergencies. The latter practice is generally known as '**data philanthropy'**.[97] Between 2008 and 2015, for instance, Google shared data concerning potential 'flu' outbreaks in the USA with public health institutions, to anticipate new 'flu' outbreaks in specific geographical areas.[98] Google could elaborate such data on the basis of the search queries typed in by its users in specific geographical areas. Before a 'flu' outbreak, Internet users were usually searching on Google information for information relating to 'flu' synthons and possible remedies. During the COVID-19 pandemic, several digital platforms have followed a similar pattern, sharing their datasets with public institutions. Similarly to the models described above, data philanthropy takes place via an open access regime, mostly via data re-use; it is the model that most characterizes B2G data sharing.

Open data, civic data sharing, data prizes/awards and data philanthropy are emerging models in B2G and G2B data sharing, in addition to the traditional models that are based on compensation, such as data platforms, marketplace and technical enabler. As mentioned in relation to B2B, it is difficult to categorize these models, which are continuously evolving, following technological development and the spreading of data sharing practices.

2.4. Benefits of data sharing

As mentioned in the introduction, data represents an essential input in the context of the digital economy. First, data sharing improves the efficiency of the recipient undertaking: by improving its understanding of the consumers' demands, the recipient firm can develop more personalized products, and market them via targeted advertising.[99] Data sharing therefore improves the ability of the recipient firm to innovate, in terms of new products released on the market and/or the improvement of existing ones so that they are available in a more personalized way. Secondly, by analysing customers' data, a firm can also reduce its production costs: instead of cutting costs on a random basis, data analytics provide insight that allows companies to make strategic adjustments in terms of their production costs.[100] Finally, by releasing a new product on the market, the data sharing recipient undertaking may enter into a new market; in other words, data sharing stimulates the entry

95 *Supra, Supra,* 2018 European Commission Staff Working Paper on Common European Data Space, Section 4.
96 <https://data.org/organizations/mastercard/> (last accessed 28.11.2022).
97 Brice McKeever and others, Data philanthropy. Unlocking the power of private data for public good. Paper published in July 2018. The text of the study is available at: <https://www.urban.org/research/publication/data-philanthropy-unlocking-power-private-data-public-good> (last accessed 28.11.2022).
98 <https://datacollaboratives.org/cases/google-flu-trends.html> (last accessed 28.11.2022).
99 European Commission, *Study on model contract terms and fairness control in data sharing*, p. 16.
100 *Ibid*.

of innovative and efficient firms into the market, thus stimulating the overall market competition.[101]

Fostering innovation, efficiency and market competition are the main economic benefits of data sharing; they arise both in B2B and G2B data sharing scenarios. However, economic benefits are not the only justification for the current EU effort to stimulate data sharing. Increased data sharing, in fact, not only benefits private firms, but society as a whole. As was noted by the European Commission in its 2020 Data Strategy,

> "… making more data available and improving the way in which data is used is essential for tackling societal, climate and environment-related challenges, contributing to healthier, more prosperous and more sustainable societies."[102]

Firstly, increased data sharing may stimulate research, and this is the case between private firms in a B2B scenario, but also when public authorities allow private actors to access their datasets (G2B), as well as when private data holders share their datasets with public research institutions, like universities (B2G).[103] According to the EU Data Strategy, increased data sharing may also improve mobility, reduce CO2 consumptions and, ultimately, allow the EU to achieve its goal of becoming carbon-neutral by 2050.[104] For instance, by sharing real-time traffic data with car drivers, local authorities may reduce traffic in our cities, as well as pollution. B2B and G2B data sharing may also improve manufacturing and production processes, limiting the use of energy and natural resources. For example, in the agricultural sector, public authorities may help farmers to reduce water and fertilizer waste by sharing meteorological data and observations. Finally, increased data sharing may also contribute to the prevention, diagnosis, and treatment of diseases.[105] From this point of view, COVID-19 has resulted in a 'fundamental overhaul', stimulating both B2B data sharing between pharmaceutical companies, and G2B and B2G data sharing. The increased data sharing has helped pharmaceutical companies to develop and test new vaccines and medical treatments thus contributing to reducing the duration of the pandemic.[106]

Research, climate, mobility, agriculture, and health care are a few examples of areas in which increased B2B, G2B and B2G data sharing allows the achievement of certain public interest goals. As mentioned in the introduction, the EU Commission has identified 10 Common European Data Spaces, where an increased degree of data sharing between public and private actors might allow the achievement of certain public policy objectives.[107]

2.5. Obstacles to data sharing – the need for EU regulatory intervention

The next sub-section discusses the obstacles to data sharing, in terms of technical barriers, market failures and the lack of trust. As mentioned in the introduction, technical barriers are mostly tackled by the Common European Data Spaces project, rather than by the new cross-sectoral EU regulatory framework on data sharing. The discussion on technical barriers will therefore be rather short, while a deeper analysis will be devoted to the market failures and the lack of trust, which are the main justifications for the emerging EU regulatory framework on data sharing.

101 *Ibid*.
102 *Supra,* EU Commission Data Strategy, p. 3.
103 *Supra,* Tombal (2022), para. 93.
104 *Supra,* EU Commission Data Strategy, Section 4.
105 *Supra,* Tombal (2022), para. 93.
106 *Supra,* Tombal (2022), para. 93.
107 *Supra,* 2022 EU Commission working document on Common European Data Spaces.

2.5.a. Technical barriers

According to a survey conducted by the EU Commission in 2018, technical obstacles represent the main barrier to B2B data sharing,[108] and they are likely to have a negative effect on G2B and B2G data sharing too. The main technical barrier is the lack of '**interoperability'** among different datasets. The lack of interoperability is a key problem in the ICT industry: without interoperability, different electronic devices cannot 'talk to each other' - e.g., mobile phones produced by different manufacturers can communicate because of common industry standards. In the context of the data economy, a lack of interoperability means that, even if the data holder agrees to share data with a third party in real-time, via a cloud-based solution, the recipient would not be able to gain access to the cloud, and thus to importing the dataset.[109]

In addition to the lack of interoperability, data sharing may be limited by the lack of '**compatibility'** among the different datasets.[110] For instance, the data holder may collect and classify data in accordance with metadata which are not recognized by the data recipients. The different degree of 'granularity' of the datasets (i.e., the degree of data details) and potentially missing data, are also factors that are obstacles to the technical compatibility among different datasets.[111] While the lack of interoperability limits the sharing process, the lack of compatibility limits the ability of the data recipient to integrate the received data with their own dataset. Finally, **security** considerations may also undermine the data holder's incentives for sharing the data.[112] This is the case especially for the real-time and question-and-answer data sharing modalities, which are discussed in Section 2.3. In both scenarios, in fact, the recipient directly gains access to the data via a cloud solution; the recipient thus gets direct access to the data holder's IT system, thus potentially creating cybersecurity risks for the data holder's IT system.

Although technical barriers are widespread in the data economy, they may be solved only via *ad hoc* industry solutions. As discussed in Section 2.4, sharing platforms and technical enablers may design common Application Programming Interfaces (APIs) to facilitate the data exchange between the data holders and the recipients. Similarly, platforms and technical enablers can also harmonize the format of the metadata and prevent cyber-security risks. Since technical barriers may be solved only via *ad hoc* industry solutions, the EU legislator has decided to tackle these issues in the context of the Common European Data Spaces, rather than via the emerging cross-sectoral EU regulatory framework, discussed in the present paper.[113] When established, the Data Spaces should solve the technical and security issues undermining data sharing in each industry. The recently established Data Spaces Support Centre (DSSC) will have the task of facilitating the elaboration of common industry standards to facilitate the sharing process.[114]

108 *Supra,* European Commission Study on data sharing between companies in Europe, p. IX.
109 *Supra,* European Commission Study on data sharing between companies in Europe, p. 25.
110 *Supra,* Gal and Rubinfeld, p.747.
111 *Supra,* Gal and Rubinfeld, p.747.
112 *Supra,* European Commission Study on data sharing between companies in Europe, p. 44.
113 <http://dataspaces.info/#concepts> (last accessed 28.11.2022).
114 <https://dssc.eu/> (last accessed 28.11.2022).

2.5.b. Market failures

From an economic perspective, data is characterised by specific features, which have an impact on the sharing process. First, data is '**non-rival'**: many parties can use the same dataset for different purposes without creating any value loss for the original data collector.[115] Similarly, users can provide their data to multiple actors.[116] The latter is a major difference in comparison to 'physical' factors of production, which usually cannot be used by multiple parties at the same time. The non-rival nature of data has important legal implications: as recognized by the proposed Data Act,[117] data cannot be subject to any *sui generis* IP right; rather than transferring the ownership of its dataset, in fact, the data holder grants either 'access' or 're-use' to a third party, without losing the right to the continuing use of the same dataset.

Secondly, data is characterised by important **economies of scale and scope**: the larger the amount and variety of the data collected, the better the accuracy of the AI predictions are, thus improving the quality of the digital service provided to consumers. According to Prüfer and Schottmüller,[118] this mechanism causes '**indirect network effects'**: the improved quality of the digital service, in fact, attracts further users, who feed the algorithm with further data (i.e., the user feedback loop), thus self-reinforcing the economies of scale. Secondly, the larger number of users also increases the firm's revenues (e.g., a larger number of users increases the advertising revenues for social media and search engines).[119]

Thirdly, data may be defined as an '**infrastructural resource'**:[120] data is not an end-user product as such, but is, rather, an input that produces different types of services and improves the quality of goods. A dataset is simply a compilation of different data, which does not have any economic value as such. However, as discussed in the previous section, firms can rely on data to improve the quality of their services, as well to cut their production costs. In the context of the digital economy, having access to certain datasets is essential for certain firms in order that they can remain competitive in the market. As Tombal argues, although data is non-rival and not subject to property rights, "in practice, data may be technically and contractually **excludable**." – i.e., the data holder may exclude third parties from having access to the data.[121] The large economies of scale and scope, as well as the indirect network effects, are major entry barriers that cause market concentration. In the context of the digital economy, data is controlled by few large incumbent data holders, which seem to be reluctant to share their datasets with third parties.[122]

As noted by a 2022 EU Commission study, two market failures may undermine B2B data sharing. On the other hand, when a single incumbent controls access to '**critical data'** (i.e., data that is essential for the business models of certain firms, which cannot be replaced by comparable data), the incumbent may have an incentive to exclude competitors from getting access to the data by refusing to conclude a data sharing agreement.[123] On the other hand, even when access is granted, the incumbent may have an incentive to impose unfair and discriminatory conditions on the data

115 Charles Jones, Christopher Tonetti (2020), *Nonrivalry and the Economics of Data.* Volume 110, issue 9 *American Economic Review:* 2819-2858.

116 The expression 'multi-homing' generally refers to the ability of users to provide their personal data to multiple online platforms to receive different digital services.

117 "In order to realize the important economic benefits of data as a non-rival good for the economy and society, a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use."
Supra, para. 6, preamble, proposed Data Act.

118 Jens Prüfer, Christoph Schottmüller (2021), 'Competing with Big Data' Vol 64, issue 4 *Journal of Industrial Economics:* 967-1008.

119 Jan Krämer, Daniel Schnurr, Sally Broughton Micova, *The role of data for digital markets contextability: case studies and data access remedies.* CERRE report, published in September 2020. The report is available at: <https://cerre.eu/publications/data-digital-markets-contextability-case-studies-and-data-access-remedies/> (last accessed 9.8.2022).

120 Christian Reimsbach-Kounatze, 'Enhancing Access to and Sharing of Data: Striking the Balance between Openness and Control over Data.' In Federal Ministry of Justice and Consumer Protection & Max Planck Institute for Innovation (eds.), Data Access, Consumer Interests and Public Welfare (Nomos, 2021), pp. 27-68. At 31.

121 *Supra,* Tombal (2022), p. 43.

122 Thomas Tombal (2022), "The rationale for compulsory B2B data sharing and its underlying balancing exercises." 84 *Revue du Droit des Technologies de l'information:* 5-26.

123 *Supra,* European Commission, *Study on model contract terms and fairness control in data sharing*, p. 7.

recipients.[124] These market failures resemble the refusal to deal/essential facility doctrine under EU competition law. However, most scholars agree that Art. 102 TFEU could hardly be used to sanction a refusal to grant access to data.[125] Firstly, the data incumbent may have a strong bargaining position at a bilateral level, but it would not necessarily be 'dominant' in the relevant market in which it operates. In addition, conditions for the application of the essential facility doctrine can hardly be met in such a hypothetical case: first, the access denial may lead to the firm requesting the data to drop out of the market, but it would not be "likely [to] eliminate all competition" in the relevant market.[126] Secondly, due to the data's non-rival nature and the lack of exclusive ownership rights, it would be hard to argue that dataset replication is "impossible"[127] – i.e., it might be extremely costly and complicated, but is not impossible. Finally, it is doubtful that the "new product" condition would be satisfied[128] – i.e., the requesting firm might need the data either to improve the quality of its products or to improve the efficiency of its production and supply chain, rather than to release a new product in the market.

To sum up, although data is non-rival and is not subject to exclusive ownership rights, its collection generates network effects that lead to market concentration. Although data sharing might foster innovation and facilitate the entry of new firms into the market, data incumbents might be reluctant to engage in B2B data sharing, which may undermine their market position. Refusal to grant access to the dataset / access under unfair conditions is a market failure that may undermine B2B data sharing. Since Art. 102 is generally considered unsuitable for solving these market failures, the EU legislator has opted for *ex-ante* regulation to solve them. As further discussed in Section 3, the mandated data access that is included in the DMA and in the sector-regulation aims to force the data holder to provide access to its dataset for its competitors, and, by doing so, thus solving these market failures.

Even in the absence of a data holder's strategic behaviour to undermine the data sharing process, the data holder may not have sufficient 'incentives' to encourage them to share the data.[129] As mentioned in the introduction, with the lack of a functioning market, firms may not be aware of the value of their dataset and thus they will not share their data.[130] The **lack of economic incentives** may affect B2B, as well as G2B, transactions that take place via a data platform, marketplace or technical enabler -i.e., G2B data sharing based on an economic rationale, as B2B data sharing. By contrast, other typologies of G2B and B2G data sharing, such as open data, civic data sharing, data prizes/awards and data philanthropy, may not be affected by the lack of economic incentives, since the data holder allows the data's re-use to achieve an objective that is of general interest, rather than looking for compensation. The new EU regulatory framework has introduced general rules on compensation to solve the incentive problem. Since the degree of compensation varies, depending on the data's quality, and their value in both the supply chain and industry practices, the EU legislator has provided only general rules on compensation. As further discussed in Section 3, it is up to the parties to define the precise value of compensation in each transaction.

Finally, high **'transaction costs'** and '**information asymmetries** might also represent market failures that undermine the data sharing process. The expression transaction costs generally refers to the costs faced by the parties in order to engage in the transaction – e.g., the seller has to spend time looking for a buyer, while the buyer makes an effort to look for a seller.[131] On the other hand, the expression 'information asymmetries' generally refers to an imbalance in the ability of the buyer and seller to gain access to product information.[132] Information asymmetries create an imbalance

124 *Supra,* European Commission, *Study on model contract terms and fairness control in data sharing*, p. 7.
125 *Supra*, Drexl (2016), p.44.
126 Case C-7/97, *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs* (1998) ECLI:EU:C:1998:569. para. 41.
127 *Ibid,* para. 41.
128 Case C-241/91*, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission* (1995) ECLI:EU:C:1995:98, para. 29.
129 Bertin Martens, Néstor Duch-Brown, The economics of Business-to-Government data sharing. JRC Digital Economy Working Paper 2020-04. Section 3.3.2. The report is available at: <https://joint-research-centre.ec.europa.eu/publications/economics-business-government-data-sharing_en> (last accessed 30.11.2022).
130 *Supra,* Reimsbach-Kounatze, p. 43.
131 OECD Glossary of Statistical Terms, available at: <https://stats.oecd.org/glossary/detail.asp?ID=3324> (last accessed 30.11.2022).
132 Hayne E. Leland, David H. Pyle (1977), "Informational Asymmetries, Financial Structure, and Financial Intermediation." 32(2) *The*

between the seller and the buyer in relation to their bargaining positions, and this is an imbalance which usually favours the seller. For instance, the owner of a car usually has better information about the quality of his/her car than a potential buyer. Transaction costs and information asymmetries are also common in the data economy:[133] When there is the lack of a functioning data market, a potential buyer may have problems in identifying a suitable data provider, while a data supplier faces the challenging task of looking for an interested buyer. Similarly, since every dataset has features that are almost unique, it is rather difficult for a buyer to identify the dataset for which he/she is looking. Data platforms, marketplaces, and technical enablers, improve the match between a buyer's demands and the seller's supply, thus reducing information asymmetries and transaction costs. From a regulatory perspective, the Common European Data Spaces announced by the EU Commission also aim to reduce transaction costs and information asymmetries:[134] in each data space, in fact, data providers and suppliers will gain better access to information. These market failures, therefore, will be tackled by future sector regulation, rather than by the overall EU data sharing legal framework that is discussed in this present paper.

To sum up, strategic refusal to give access to critical data, a lack of economic incentives, high transaction costs and information asymmetries are the main market failures that affect the data sharing economy. The EU legislator is currently tackling these barriers via different tools, while mandated sharing tackles the strategic refusal to share data by the data holder, the rules on compensation tackle the problems caused by a lack of incentives. Finally, the Common European Data Spaces act as matching platforms in certain industries, thus reducing transaction costs and information asymmetries.

2.5.c. Lack of trust

Market failures and technical barriers are not the only factors that undermine data sharing. The 'lack of trust' in the data sharing process is an additional factor that undermines the data holder's incentives to share its dataset. Lack of trust may be caused by several issues. First, a lack of trust may be caused by the '**lack of experience'** of the data holder in relation to the data sharing process. Data sharing is a rather new socio-economic phenomenon. Business operators, especially SMEs, still lack familiarity with B2B data sharing, since they have never previously engaged in this type of transaction.[135] Similarly, public institutions may be unaware of the public interest goals that they can achieve via open access data re-use.[136] Finally, business operators that collect a large amount of data may be unaware of the possibility of sharing their data with public institutions in the context of data prize/awards or data philanthropy.[137] Via the spread of data sharing, a larger number of public and private actors have become familiar, and thus less sceptical, about this process.

Secondly, a lack of trust in data sharing may also be caused by a '**reputational risk',** a risk that is mostly perceived by business operators when sharing personal data.[138] Some business operators, in fact, may be concerned about losing their reputation if their consumers discover that their data, even if anonymized, have been shared with third parties. During recent years, the EU Data Sharing Support Centre (DSSC) has engaged in data sharing advocacy[139] via the organization of conferences, thematic workshops, studies, the elaboration of best practices and marketing materials on the benefits of data sharing, such as podcasts and flyers, the DSSC has tried to increase the familiarity of private and public institutions with data sharing benefits and has thus reduced the perceived risk of reputational loss.

Journal of Finance: 371-387.

133 *Supra,* Martens and Duch-Brown (2020). Section 2.2.

134 <http://dataspaces.info/common-european-data-spaces/> (last accessed 30.11.2022).

135 *Supra,* European Commission Study on data sharing between companies in Europe, p.. 26.

136 *Supra,* European Commission Study creating value through open data, p.

137 European Commission, Towards a European strategy on business-to-government data sharing for the public interest. Report published in 2020, p.60. The text of the report is available at: <https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1> (last accessed 28.11.2022).

138 *Supra,* European Commission Study on data sharing between companies in Europe, p. 44.

139 <https://eudatasharing.eu/> (last accessed 30.11.2022).

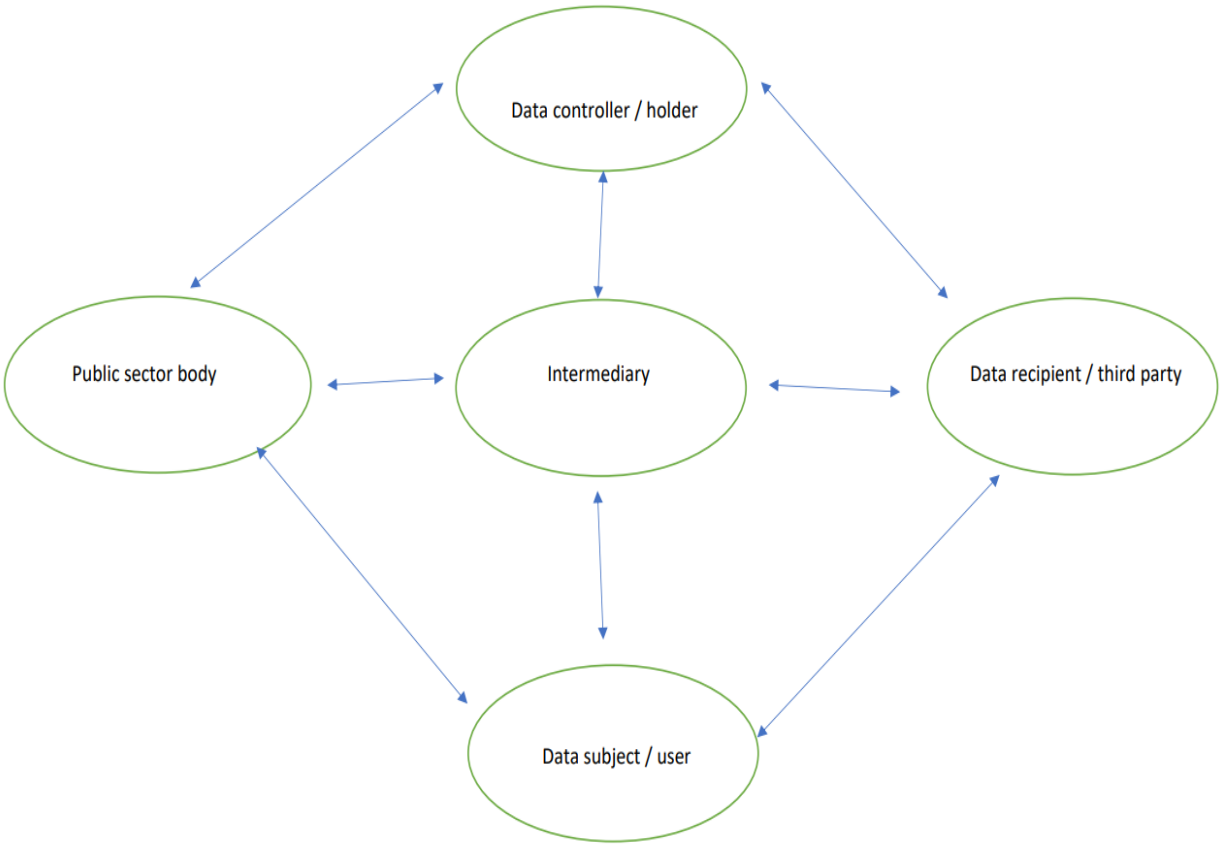
Thirdly, the lack of trust in the data sharing process may be caused by the current '**legal uncertainty'** regarding this topic. Data sharing is a rather new socio-economic phenomenon; its regulatory framework is in its 'infancy'. During recent years, EU Member States have adopted a number of laws to regulate different modalities of B2B, G2B and B2G data sharing.[140] Different national interventions may also cause legal uncertainty and restrict cross-border trade of data within the EU.[141] The recent legislative intervention by the EU legislator, which is further discussed in Section 3, aims to increase legal certainty and ti reduce the divergences among the national regulatory frameworks.

Finally, lack of trust may also be caused by specific '**legal concerns**.' Firstly, the 2018 EU Commission study on data sharing practices showed that business operators were uncertain about the ownership rights over the data that they had collected.[142] In other words, data holders may be unaware of the fact that they control a dataset, but they do not have any ownership rights that they transfer, in an exclusive manner, to a third party. Similarly, data sharing may also be affected by privacy and liability concerns.[143] The data holder may be concerned with how the recipient party will process the acquired data. In particular, the data holder may be concerned with their liability *vis-à-vis* their own consumers/users, in relation to a possible breach of data protection rules by the data recipient.[144] Once again, the EU regulatory framework, discussed in Section 3, aims to solve this problem.

To sum up, the lack of trust is a general problem that negatively affects data sharing. It includes several sociological dimensions, e.g., a lack of experience and the risk of reputational loss, as well as legal issues, such as legal uncertainty and specific legal concerns. While the sociological issues may be solved via advocacy programs to inform public and private institutions about the benefits of data sharing, the EU is trying to increase legal certainty via the common regulatory framework, which is further discussed in the pages that follow.

140 European Commission, Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access (Data Act). Brussels, 23.2.2022 SWD(2022) 34 final. Section 2.2.
141 *Ibid.*
142 *Supra,* European Commission Study on data sharing between companies in Europe, p. 45.
143 *Supra,* European Commission Study on data sharing between companies in Europe, p. 77.
144 *Supra,* Reimsbach-Kounatze, p. 40.

Figure 1: Actors involved in data sharing



Source: author's own illustration.

3. The EU legal framework on data sharing

As shown in Figure 1, data sharing is a complex process which involves a plurality of different actors, and it covers both personal and non-personal data. This section discusses the different typologies of data sharing, as regulated by the EU legal framework, focusing on the sharing conditions and remuneration.

3.1. B2B data sharing

A third typology of data sharing concerns the transaction between the data controller/holder and a third party; in the case of private parties, we can define this typology as 'B2B data sharing'.

In functioning markets, this typology of data sharing would be subject to the parties' contractual freedom. The data supplier and the recipient would define the conditions and compensation for data sharing in a contract. In the case of personal data, the transaction would take place only if one of the legal bases in Art. 6 GDPR was fulfilled (e.g., data subject provided his/her consent), or if the data were fully anonymized. However, as discussed in Section 2, B2B data sharing may be undermined by a number of technical barriers, security concerns as well as market failures. At the core of the EU legal framework, therefore, there are provisions to encourage B2B data sharing. Such provisions, which are present in the GDPR, Data Act, DMA and sector-specific regulation, may be distinguished as falling into two categories: 'data portability' and 'mandated data sharing'. While data portability is a right enjoyed by the data subject/user, who can ask the data controller/holder to transfer the data to a third party, mandated data sharing is a legal obligation for the data controller/holder. Such an obligation is usually imposed to solve market failures, such as information asymmetries and excessive data concentration. To solve such market failures, the data controller/holder is usually required to share the dataset with their competitors.

3.1.a. Data portability

Data portability is a right that can be exercised by the data subject. Under Art. 20(1) GDPR, in fact, the data subject has the right to obtain his/her personal data from the controller in a "structured, commonly used and machine-readable format", to later "transmit" such data to a different controller (i.e., a third party). In addition, under Art. 20(2) GDPR, the data subject may ask the controller to transmit his/her data directly to another controller "where technically feasible." The GDPR preamble points out that the data subject may exercise the right to data portability only in a case where the original data processing was due either to the performance of a contract, or due to the data subject's consent.[145] By contrast, data portability cannot be exercised in the case that the data controller is required by law to process the data.[146] By way of example, the user of a social media may require the platform to migrate its personal data to another social service. In practice, this possibility usually remains "largely theoretical".[147] Data portability represents one of the major novelties of the GDPR; it aims to strengthen the ability of data subjects to switch between different controllers, and thus to switch between services providers. However, data portability has rarely been exercised by any data subject. As discussed in the previous section, interoperability represents a major obstacle to B2B data sharing; data portability becomes ineffective with the lack of common technical standards.[148]

Although the expression 'data portability' usually refers to the data subject's right under Art. 20 GDPR, the proposed Data Act includes a similar user's right to portability in relation to the non-personal data generated by a product's use. In particular, the user may ask the data holder to make the data available, "where applicable" to a third party "continuously and in real-time."[149] The recipient cannot further share the data with any another third party,[150] neither can that recipient use the received data to develop products that compete with those of the data holder.[151] Finally, the proposed Data Act provides that a digital gatekeeper, within the scope of the DMA, may not be considered an eligible data recipient, in order to prevent the further strengthening of its market position.[152] By contrast, data holders that qualify as Small and Medium Enterprises (SMEs) are not requested to share data with third parties, while they can qualify as data recipients.[153]

According to Habic, the data portability regime introduced by the proposed Data Act is positive for all the stakeholders who are involved in the process,[154] on the one hand, the users can access to the data he/she has generated via the product's use, free of charge.[155] On the other hand, the data holder may rely on the generated data to improve the quality of a product; in this case, it would be asked by the user to grant access to the dataset to a third party, and it could ask for compensation on a FRAND basis, and it would still have access to the dataset.[156] Finally, the recipient may benefit from the shared data.

The GDPR and the proposed Data Act radically diverge in terms of compensation for data portability. On the one hand, under the GDPR, data portability is considered a 'right', which can be exercised 'free of charge' by the data subject.[157] The GDPR provides for an exception to this regard:

145 *Supra,* para. 68, preamble GDPR.
146 Ibid.
147 *Supra,* Impact assessment Data Act proposal, p.. 4.
148 *Ibid*.
149 *Supra,* Art. 5(1) proposed Data Act.
150 *Supra,* Art. 6(2)(c) proposed Data Act.
151 *Supra,* Art. 6(2)(e) proposed Data Act.
152 *Supra*, Art. 5(2) proposed Data Act.
153 *Supra,* Art. 7 proposed Data Act.
154 *Supra,* Habic, p. 1349.
155 *Supra,* Art. 4(1) proposed Data Act.
156 *Supra,* Art. 8 proposed Data Act.
157 *Supra,* Art. 20 GDPR.
Graef, Musovec and Purtova have pointed out that it is not clear, from the text of Art. 20 GDPR, whether reuse of ported data by receiving parties is also free of charge when data is protected by IP rights (e.g., copyright, trademark).

in case the portability request is "manifestly unfounded or excessive",[158] especially of its "repetitive character", the controller may either reject the portability request or charge a "reasonable fee", covering the costs faced in implementing the portability request. On the other hand, the proposed Data Act points out that the data holder should share the data with a third party, identified by the user, on the basis of FRAND conditions,[159] and such conditions should be specifically defined in a contract concluded between the data holder and the third party.[160] The compensation for data sharing should be "reasonable".[161] The Data Act's preamble points out that, in a case where data sharing involves "large companies", the recipient would be considered "capable" of assessing whether the compensation is indeed "reasonable", taking in consideration the volume, format, nature, demand and costs faced by the holder for sharing such data.[162] The data holder should inform the recipient about the criteria used to calculate the compensation, so that the recipient may verify whether the required compensation is indeed reasonable.[163] Finally, the Data Act reserves the possibility for the EU legislator to introduce, in separate legislation, a "lower compensation" for sharing specific categories of data.[164]

According to Monti, Tombal and Graef, the Data Act proposal grants a remuneration to the data holder to incentivize its efforts to collect and systematize the data.[165] According to the authors, the remuneration should cover the sharing costs faced by the data holder and a 'plus' elements. The "costs" should include the technical costs faced by the data holder to make the requested data available (i.e., compiling, storage and formatting), the human and organizational costs faced in arranging the data sharing process.[166] By contrast, the data collection costs initially faced by the data holder should not be taken in consideration.[167] The 'plus' element implies a degree of profit for the data holder, which should be assessed on the basis of the amount and quality of shared data (e.g. whether the shared data are raw or inferred by the data holder), whether the initial data collection was at the core of the data holder's business model, rather than a side product of its business, and what is the follow-on use of the shared data.[168] While Monti, Tombal and Graef seem to support the idea that B2B data sharing should be remunerated, the compensation mechanism introduced by the Data Act has been criticized by Kerber:[169] the author believes that compensation would not be needed, since the data controller would have enough incentives to continue collecting data, even in case it was forced to share data deriving from the product use. In addition, the third party receiving the data would likely pass the cost of compensation to final consumers, by thus defeating the legislator's intention to safeguard a free access to data for final users. The Data Act is currently a legislative proposal; the compensation is one of the most controversial aspects of the proposed legislation.

The Data Act also spells out the meaning of FRAND in relation to the possible discrimination against different data recipients. In particular, the data holder should not discriminate "between comparable categories of data recipients."[170] In the case of alleged discrimination, the data holder will have to prove that it has treated different recipients in a similar way - i.e., there is a reversed burden of proof relating to discrimination.[171]

Inge Graef, Martin Husovec, Nazehda Purtova (2019), 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law.' 19(6) *German Law Review:* 1384.

158 *Supra,* Art. 12(5) GDPR.

159 *Supra,* Art. 8(1) proposed Data Act.

160 *Supra,* Art. 8(2) proposed Data Act.

161 *Supra,* Art. 9(1) proposed Data Act.

162 *Supra,* para. 46, preamble to proposed Data Act.

163 *Supra,* Art. 9(4) proposed Data Act.

164 *Supra,* Art. 9(3) proposed Data Act.

165 *Supra*, Monti, Tombal, Graef, p. 2.

166 *Supra,* Monti, Tombal, Graef, p. 12-15.

167 *Supra,* Monti, Tombal, Graef, p. 12-15.

168 *Supra,* Monti, Tombal, Graef, p. 20-25.

169 Wolfgang Kerber (2023), 'Governance of IoT Data: Why the EU Data Act Will Not Fulfill its Objectives.' 72(2) *GRUR International:* 120-135.

170 *Supra,* Art. 8(3) proposed Data Act.

171 Ibid.

The Data Act also includes specific provisions for the facilitating of data sharing with SMEs. First of all, in a case where the beneficiary was a SME, the compensation for data sharing should not exceed the "direct costs" faced by the data holder in order to arrange the transaction.[172] According to the Data Act's preamble, the direct costs include the "costs necessary for data reproduction, dissemination via electronic means and storage, but not of data collection and production."[173] Due to the principle of non-discrimination, mentioned above, different SMEs would be expected to pay the same price to access the same dataset, since they would be considered "comparable categories of data recipient."[174] In addition, the Data Act points out that contractual terms "unilaterally imposed"[175] by the data holder to SMEs would be considered 'unfair' if they "grossly deviate from good commercial practices".[176] Art. 13 of the Data Act includes a list of clauses that are *per se* considered to be unfair,[177] as well as clauses that are "presumed" to be unfair (i.e., rebuttable presumption).[178] Individual unfair clauses would be considered null and void.

Finally, the Data Act provides for the establishment of new dispute settlement bodies, to solve disputes between the data holder and a third party in relation to the determination of FRAND conditions.[179] The bodies should be established in every Member State, "impartial and independent", and subject to "clear and fair rules of procedures." [180] The bodies should be accessible via electronic communications,[181] and they should be able to solve the dispute "in a swift, efficient and cost-effective manner" (i.e., within 90 days).[182] The decision adopted by the new dispute settlements bodies does not prevent the right of the parties to seek judicial redress in the national courts of EU Member States.[183]

The provisions discussed above represent one of the major innovations of the proposed Data Act. They aim to encourage B2B data sharing to the benefit of SMEs, while preventing digital gatekeepers from further strengthening their market positions by acting as data beneficiaries. The meaning of FRAND, in the context of the Data Act, will be further discussed in Section 4, when it is compared to the application of the FRAND principle in the context of SEP disputes and competition law remedies.

Data portability has also been strengthened by the Digital Markets Act. Art. 6(9) DMA introduces an unconditional obligation for the gatekeeper to guarantee the portability of the collected data on the core platform service.[184] In particular, the data should be shared "in real-time" with third parties.[185] According to the DMA preamble, the new obligation complements the right to data portability under the GDPR, "facilitating switching and multihoming" for end users.[186] Since Art. 6(9) DMA refers to "data", the new data portability right covers both personal and non-personal data, and the DMA thus bridges the current distinction between the legal regimes that now exist under the GDPR and the proposed Data Act . On the other hand, unlike the proposed Data Act, the DMA points out that the gatekeeper will not receive any compensation when the end user decides to exercise its right to data portability, even when the gatekeeper is required to transfer the data to one of its competitors.

172 *Supra*, Art. 9(2) proposed Data Act.
173 *Supra,* para. 45, preamble to the proposed Data Act.
174 *Supra,* Art. 8(3) and Art. 9(2) proposed Data Act.
175 "A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content, despite an attempt to negotiate it."
Supra, Art. 13(5) proposed Data Act.
176 *Supra,* Art. 13(2) proposed Data Act.
177 *Supra,* Art. 13(3) proposed Data Act.
178 *Supra,* Art. 13(4) proposed Data Act.
179 *Supra,* Art. 10(1) proposed Data Act.
180 *Supra,* Art. 10(2)(a) proposed Data Act.
181 *Supra,* Art. 10(2)(c) proposed Data Act.
182 *Supra,* Art. 10(2)(d) and Art. 10(7) proposed Data Act.
183 *Supra,* Art. 10(9) proposed Data Act.
184 *Supra,* Art. 6(9) DMA.
185 *Supra,* Art. 6(9) DMA.
186 *Supra,* para. 59, preamble DMA.

3.1.b. Mandated B2B data sharing

Data portability is a right that is enjoyed by the data subject/user; consequently, B2B data sharing can be triggered only upon the request of the right holder. As mentioned in the previous section, the proposed Data Act points out that the recipient may not use the shared data to develop products that are in competition with those of the data holder. By contrast, 'mandated' B2B data sharing refers to an obligation, on the part of the data controller/holder, to share data with third parties, which are usually its competitors.

Mandated data sharing in the DMA

The Digital Markets Act (DMA) includes a set of obligations that are applicable to those 'core platform services' that fulfil certain thresholds (i.e., in terms of the number of users and turnover) so that they can be considered 'gatekeepers', and are thus subject to the DMA obligations.[187] The DMA aims to ensure 'fairness' and 'contestability' in digital markets.[188] To achieve the market contestability goal, the DMA includes three B2B data sharing obligations, which are aimed at encouraging the entry of new players into the market.

Firstly, gatekeepers that operate in the field of digital advertising (e.g., social networks, search engines) shall provide, to advertisers and publishers, access to the performance measuring tools relied upon by the gatekeeper, as well as to the data necessary to measure the effectiveness of such tools.[189] The objective of this data sharing obligation is to increase market transparency:[190] advertisers can compare the advertising costs with the remuneration granted by the gatekeeper to different publishers, so that advertisers can compare the offers provided by different platforms. Such increased transparency will also benefit publishers, who will be able to compare the potential advertising revenues granted by different platforms.

Secondly, gatekeepers should provide, to business users and to third parties, access to the data generated by consumers, in the context of the use of the core platform service.[191] For instance, business users selling products on Amazon marketplace should receive access to the data generated by the final consumers, while purchasing products on Amazon. The data sharing obligation aims to prevent gatekeepers, like Amazon, from benefiting from preferential access to consumers' data due to their 'dual role' – i.e., as a platform operator and, at the same time, as a competitor, with business users relying on the platform to sell products.[192] Art. 6(10) DMA points out that the data sharing obligation covers both "aggregated and non-aggregated data, including personal data." Personal data should be shared by the gatekeeper with business users only if that data is "directly connected" with the products purchased by the consumer and provided that the consumer has provided his/her consent to such sharing.[193] Finally, data sharing should comply with specific quality standards; data sharing, in fact, should be "effective, high-quality, continuous and in real-time."[194]

Thirdly, gatekeepers that are active as online search engines must provide to competitors access to the "query, click and view data" that is generated by final users.[195] The gatekeepers shall share such data upon the request of the competitor. In the case that the shared data includes personal data, the latter shall be anonymised by the gatekeeper,[196] in such a way as to avoid any possible risks of the re-identification of the data subject.[197]

187 *Supra,* Art. 3 DMA.
188 "…the purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down rules to ensure contextability and fairness for the markets in the digital sector…"
Supra, para. 7, preamble DMA.
189 *Supra,* Art. 6(8) DMA.
190 *Supra,* para. 45, preamble DMA.
191 *Supra,* Art. 6(10) DMA.
192 *Supra,* para. 46, preamble DMA.
193 *Supra,* Art. 6(10) DMA.
194 *Supra,* Art. 6(10) DMA.
195 *Supra,* Art. 6(11) DMA.
196 *Supra,* Art. 6(11) DMA.
197 *Supra,* para. 61, preamble DMA.

The three data sharing obligations aim to 'cure' specific cases of excessive data concentration, usually affecting digital markets. It is worth bearing in mind that these mandated data sharing obligations are included in Art. 6 DMA: their precise scope of application (e.g., the definition of the data recipients; the modality of sharing) will be further defined by the EU Commission decision which imposes specific obligations on those firms with gatekeeper status.[198] Thee three obligations require the gatekeeper to share the data both with 'direct competitors' (e.g., a competing search engine) and third parties, using the platform ecosystem (e.g., advertisers, publishers and business users selling products on the platform marketplace). Secondly, the obligations underline the importance of 'real-time' data access. In terms of compensation, the gatekeeper shall share the data "free of charge" with advertisers/publishers/business users. The only exception is represented by search engines, which shall share the query data with other search engines (i.e., 'direct competitors') based on FRAND conditions.[199]

Mandated data sharing by sector-specific regulation

The DMA is not an isolated example of mandated data sharing in a specific sector. During recent years, mandated data sharing has been introduced in several EU Regulations and Directives.

The first example of B2B mandated data sharing can be found in the EU Regulation on Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH).[200] One of the objectives of the Regulation is to stimulate the sharing of previous tests carried out by firms operating in the chemical sector, in order to limit the number of experiments with chemical substances on animals.[201] REACH identifies 2 typologies of data sharing: on the one hand, the firm requesting the registration of a new chemical substance can ask a previous registrant for access to data involving previous tests on animals.[202] Both the data holder and the potential recipient will 'make every effort' to reach a data sharing agreement.[203] The cost of data sharing should be determined in a fair, reasonable and non-discriminatory way.[204] Reference to a FRAND basis is also present in Art. 303, REACH: the latter provision requires the firm that has registered a substance via the Substance Information Exchange Forum (SIEF) to share data concerning previous tests carried out on animals with potential registrants on a FRAND basis.

While the objective of mandated data sharing under REACH aims to achieve a public interest goal (i.e., safeguarding animals' welfare), data sharing obligations under other EU legislation aims to solve market failures, such as information asymmetries and excessive data concentration, to stimulate the entry of new competitors into the market. A well-known example, in this regard, is the second Payment Service Directive (PSD2).[205] The latter legislation, adopted in November, 2015, introduced the Access to the Account (XS2A) rule,[206] in order to stimulate the entry of FinTech operators into the banking sector and thus stimulating competition in the industry.[207] According to the XS2A rule, commercial banks should provide access to data on users' accounts to Third Party Providers (TPPs), as well as providing access to such accounts by executing payment orders.[208] The XS2A rule is applicable only in the case of online bank accounts,[209] and in a case where the consumer has provided his/her "explicit consent" to such data sharing,[210] since the latter involves personal data.

198 *Supra,* Art. 8 DMA.
199 *Supra,* Art. 6(11) DMA.
200 Supra, REACH.
201 *Ibid,* Art. 25 REACH.
202 *Ibid,* Art. 27 REACH.
203 *Ibid,* Art. 27(3) REACH.
204 *Ibid,* Art. 27(3) REACH.
205 *Supra*, Directive 2015/2366.
206 *Supra,* Art. 67 Directive 2015/2366.
207 Oscar Borgogno, Giuseppe Colangelo (2020), 'The Data Sharing Paradox: BigTechs in Finance' 1 Vol. 16, Issue 2 *European Competition Journal:* 492-511.
208 *Supra,* Art. 67 Directive 2015/2366.
209 "That right shall not apply where the payment account is not accessible online." *Supra,* Art. 67(1) Directive 2015/2366.
210 *Supra,* Art. 67(2)(a) Directive 2015/2366.

According to Feasy and De Streel, XS2A strengthens data portability if compared to Art. 20 GDPR:[211] data portability under the XS2A is unconditional, and it should take place on a continuous / real-time basis. The PSD2 points out that banks should grant data access to other financial operators 'without any discrimination.'[212] On the other hand, PSD2 does not provide any detail on whether data access should occur free of charge, or whether it should be subject to reasonable compensation. We might thus define this data sharing framework as 'quasi-FRAND'.

A third example of B2B mandated data sharing can be found in the 2018 Motor Vehicles Regulation.[213] According to Art. 61, car manufacturers should provide access to independent operators to 'vehicle on-board diagnostic' (OBD) data.[214] Similarly to the XS2A rule, the access rule aims to encourage consumers to rely on the repair services offered by independent mechanics (i.e., who are competitors of the data holders), so that the consumers are not tied to the repair services provided by the car manufacturer. Taking into consideration the increasing amount of diagnostic data collected nowadays by cars, it is, in fact, important for independent operators to have access to such non-personal data to provide their repair services. According to the Motor Vehicles Regulation, the car manufacturers shall provide data to the independent mechanic in an "easily accessible manner in the form of machine-readable and electronically processable datasets".[215] In terms of remuneration, the Motor Vehicles Regulation points out that the car manufacturer may charge a "reasonable and proportionate fees for access";[216] and such a fee may be calculated either on a time-basis (i.e., how long the mechanic had access to the dataset), or on a transaction-basis (i.e., the mechanic pays a fee each time s/he needs access to ODB).[217] Finally, the data should be provided 'on a non-discriminatory basis.'.[218]

A fourth example of mandated data access can be found in the 2019 Electricity Directive.[219] In order to ensure competition in the retail market, but also to enable new emerging services, the eligible parties must be provided with access to data. Such data and information must be shared among the consumers, networks, systems, and different applications. For example, Distribution System Operators (DSOs) and suppliers have to have access to "metering and consumption data" in order to provide network management and supply services.[220] Since personal data is involved, the data sharing for other services may take place only in compliance with the GDPR requirements (e.g., the consumer has provided his/her consent to data sharing).[221] The Electricity Directive points out that data sharing should take place in a "non-discriminatory manner and simultaneously" (i.e., multiple electricity suppliers can have access to the metering data).[222] In addition, the Directive points out that access to data 'shall be easy' and the relevant procedures to access data shall be publicly available.[223] On the other hand, final consumers should have access to the metering data "without any additional cost" (i.e., free of charge).[224] Unlike the proposed Data Act, the Electricity Directive does not mention explicitly a right to data portability for final users in relation to their metering data. In addition, except for the non-discriminatory obligation, the Directive does not include any rule on data sharing compensation. According to Art. 23(5), in fact, the energy regulatory authorities of the EU Member States shall be responsible 'for setting the relevant charges for access to data by eligible

211 *Supra,* Feasy and De Streel (2020), p.49.
212 *Supra,* Art. 67(3)(b) Directive 2015/2366.
213 *Supra,* Regulation 2018/858.
214 "Vehicle on-board diagnostic (OBD) information means the information generated by a system that is on board a vehicle or that is connected to an engine, and that is capable of detecting a malfunction, and, where applicable, is capable of signalling its occurrence by means of an alert system, is capable of identifying the likely area of malfunction by means of information stored in a computer memory, and is capable of communicating that information off-board."
Supra, Art. 3(49) Regulation 2018/858.
215 *Supra,* Art. 61(1) Regulation 2018/858.
216 *Supra,* Art. 63(1) Regulation 2018/858.
217 *Supra,* Art. 63(2) Regulation 2018/858.
218 *Supra,* Art. 63(7) Regulation 2018/858.
219 *Supra,* Directive 2019/944.
220 *Supra,* Art. 23(1) Directive 2019/944.
221 *Supra,* Art. 23(3) Directive 2019/944.
222 *Supra,* Art. 23(2) Directive 2019/944.
223 *Supra,* Art. 23(2) Directive 2019/944.
224 *Supra,* Art. 23(5) Directive 2019/944.

parties.'

Examples of mandated data sharing can also be found in the EU rules concerning the telecoms and postal sectors. According to the European Electronic Communications Code (EECC),[225] telecoms operators providing "number-based interpersonal communications services" should share data concerning telephone numbers and users with the providers of telephone directory enquiry services.[226] The data sharing should take place in accordance with "fair, objective, cost oriented and non-discriminatory" terms.[227] The European Court of Justice (ECJ) has pointed out, in *KPN Telecom,* that the costs faced by the telecom operator in compiling, updating and providing relevant information on subscribers should not represent the basis for calculating 'cost-oriented' data sharing compensation.[228] According to the ECJ, in fact, the compilation of these data is "…inextricably linked to the telephony service and does not demand any particular effort…" from the side of the telecom operator.[229] As a consequence, telecoms operators may charge, to the providers of directory enquiry services only, the 'additional costs' faced in sharing the requested data.[230]

Finally, the 2008 Postal Service Directive requires the incumbent postal operator to share data concerning the postcode, address database, post office and delivery boxes, with other postal operators.[231] The incumbent operator should provide "transparent, non-discriminatory access" to data.[232] On the other hand, the Directive does not provide for any specific remuneration for the data sharing effort.

To conclude, sector-specific regulation in the chemical, banking, automotive, electricity, telecoms and postal sectors provide for specific obligations concerning mandated data sharing: industry incumbents are usually required to share relevant data about their customers with competitors, to encourage their entry into the market (e.g., PSD2, Motor Vehicles Directive, Postal Services Directive). Alternatively, industry incumbents may be forced to share relevant data with third parties to solve an information asymmetry, and thus to enable the third party to offer a service on the market (e.g., Electricity Directive, EECC). Finally, REACH imposes data sharing in order to achieve a public interest objective: to limit experiments on animals, and by doing so, increasing animals' welfare. These examples of mandatory data sharing usually include a non-discrimination obligation, whereby the data holder cannot discriminate against the different parties that require access to the dataset. On the other hand, these rules are not coherent in relation to the conditions and level of compensation granted to the incumbent in order to compensate for the data sharing costs: the latter may be forced to share the data, either subject to a "reasonable and proportionate fee" (e.g., Motor Vehicles Directive), or subject to a "cost-oriented" fee (e.g., EECC). Finally, some legislation does not provide for any specific rules on the compensation for data sharing (e.g., PSD2 and the Postal Services Directive). Despite the industry specificities, the differences in the compensation levels are quite unsatisfactory; they show the lack of consistency in the EU regulatory framework on data sharing in relation to compensation. In addition, it remains unclear how the sector specific rules on mandated data sharing will interact, in the future, with the proposed Data Act, when the latter enters into force.

225 *Supra,* Directive 2018/1972.
226 *Supra,* Art. 112(1) Directive 2018/1972.
227 *Supra,* Art. 112(1) Directive 2018/1972.
228 Case C-109/03, *KPN Telecom BV v. Onafhankelijke Post en Telecommunicatie Autoriteit* (2004) ECLI:EU:C:2004:749.
229 *Ibid,* para. 39.
230 *Ibid,* para. 40.
231 *Supra*, Art. 11a Directive 2008/6/EC.
232 Ibid.

3.2. G2B data sharing

A fourth typology of data sharing that is regulated by the EU legal framework is represented by the flow of personal and non-personal data from national governments/public agencies to the private sector (i.e., G2B data sharing). The 2019 Open Data Directive,[233] which replaced the 2003 Public Sector Information Directive,[234] and the Data Governance Act,[235] which was approved in May 2022, are the two main pieces of EU legislation that regulate this typology of data sharing. Together, the Directive and the Regulation define a legal framework generally requiring public sector bodies to grant re-use of their data to business users.

The ODD Directive covers the sharing of "documents" held by "public sector bodies" and "public undertakings".[236] The expression 'document' is rather broad; it covers "any content whatever its medium" (i.e., including documents held in a digital format, and thus datasets held by the public administration of the EU Member States).[237] The general principle of the Directive is that public agencies should allow the "re-use" of documents, produced in the performance of their public tasks, for other commercial and non-commercial purposes, by private parties.[238] "Where possible", public sector bodies shall make the documents available in "open, machine-readable, accessible, findable and re-usable" format.[239] In general, public-sector bodies shall share the requested documents "free of charge",[240] eventually asking for the recovery of the marginal costs incurred in the "reproduction, provision and dissemination of documents as well as for the anonymisation of personal data" which is included in the document.[241] When charges are demanded, the public agency should disclose, in advance, the calculation basis for such charges.[242] The recipient should not benefit from any exclusivity right to the shared document.[243] Finally, the re-use of public documents shall be allowed in a non-discriminatory manner – i.e., the public agency should apply the same conditions of re-use (and remuneration) to comparable categories of documents and types of re-use.[244]

In addition to the general rules on the re-use of public documents, the ODD Directive includes specific rules concerning 'research data' as well as 'High Value Datasets'. Research data include statistics, the results of experiments, measurements, survey results, interview recordings and images generated by universities and other research bodies, whenever the research has been financed by public funds.[245] To stimulate the re-use of scientific data, both by other research institutions and by the private sector, the research data should be made available in accordance with the FAIR principle – i.e., Findability, Accessibility, Interoperability, and Reusability.[246] FAIR goes far beyond the general re-use principles that are included in the ODD Directive, demanding that the public sector agencies make the research data "findable" via a search database, and to allow for "interoperability" in order to share the data with other datasets. Examples of high-value datasets are geospatial, meteorological and statistics data that are held by public sector bodies.[247] Similarly to the rules on research data, public sector bodies should provide access to high-value datasets via APIs (i.e., to allow interoperability with other datasets) and ensure that the data may be downloaded 'in a

233 *Supra,* Directive 2019/1024.
234 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. OJ L-345/90, 31/12/2003.
235 *Supra,* Regulation 2022/868.
236 *Supra,* Art. 1(1) ODD Directive.
237 *Supra,* Art. 2(6) ODD Directive.
238 *Supra,* Art. 3(1) ODD Directive.
239 *Supra,* Art. 5(1) ODD Directive.
240 *Supra,* Art. 6(1) ODD Directive.
241 *Supra,* Art. 6(1) ODD Directive.
242 *Supra,* Art. 7(1) ODD Directive.
243 *Supra,* Art. 12(1) ODD Directive.
244 *Supra,* Art. 11(1) ODD Directive.
245 *Supra,* para. 27, preamble ODD Directive.
246 *Supra,* Art. 10(1) ODD Directive.
247 Annex 1 includes a list of six high-value datasets. The EU Commission, via comitology decision, extends the list of high-value datasets subject to the specific rules of the Directive.
Supra, Art. 13(2) ODD Directive.

bulk'.[248] Public sector bodies should grant access to high value datasets "free of charge",[249] with some exceptions that are related to public undertakings,[250] datasets held by libraries and museum,[251] and in a case where the data disclosure would have a "substantial impact on the budget" of the public body.[252]

In spite of the broad interpretation of the concept of documents and of the specific rules on the disclosure of research data and high-value datasets, the ODD Directive does not cover documents that are protected by IP rights held by third parties (e.g., copyright), as well as documents including personal data.[253] The DGA complements the ODD Directive, expanding data re-use to the categories of data that fall outside the scope of the Directive.[254] The conditions for the re-use of public data, mentioned by the DGA, are similar to the general conditions that are mentioned in the ODD Directive. In particular, the recipient should not be entitled to any exclusivity right on the shared data;[255] conditions for re-use shall be "non-discriminatory, transparent, proportionate and objectively justified";[256] personal data should be aggregated and anonymised before being shared.[257]

While the general re-use conditions are rather similar in the ODD and the DGA, the compensation conditions differ between the two legislations: while the Directive points out that public entities should allow the re-use of documents 'free of charge',[258] eventually asking for compensation for the marginal costs of the documents' production, the Regulation points out that public sector bodies "may charge fees for allowing the re-use of such data." The requested fee should be defined in advance (i.e., should be transparent), should be proportionate and objectively justified, and should be charged in a non-discriminatory manner among the different recipients. The DGA clarifies that the public sector agency should calculate the fee based on the costs faced in the reproduction of the data, as well as in the processes of anonymisation and the seeking of consent from the data subject. Finally, the DGA provides that public sector bodies may make the data available "at a discounted fee or free of charge" for non-commercial purposes (e.g., scientific research) or to SMEs.

The ODD and DGA diverge in relation to the compensation rules on data sharing: while, under the ODD, G2B data sharing should generally take place 'free of charge' (i.e., requesting the document disclosure costs would be an exception)[259], the DGA follows, as a general rule, the coverage of the marginal production costs;[260] by contrast, the 'free of charge' approach is rather an exception. Public sector bodies, in fact, may decide to share the data "at a discounted fee, or free of charge" in cases where the data is to be re-used for non-commercial purposes (e.g., scientific research) and if the beneficiary were an SME.[261] It is unclear if the EU legislators intentionally followed a different approach in the two pieces of legislation, either in order to generate further incentives for public sector bodies to share data under the DGA, or because 'data' sharing under the DGA would be more demanding for a public agency, if compared to 'document' disclosure under the DGA. In any case, the different compensation regime generates some degree of uncertainty, both for the public agencies and for the data recipients.

248 *Supra,* Art. 14(1) ODD Directive.
249 *Supra,* Art. 14(1) ODD Directive.
250 Public undertakings are not required to disclose high-value datasets if such disclosure would distort competition in the relevant market. *Supra*, Art. 14(3) ODD Directive.
251 *Supra*, Art. 14(4) ODD Directive.
252 In this case, the Member State may decide to exempt a public sector body from disclosing a high-value dataset for a period of up to 2 years.
Supra, Art. 14(5) ODD Directive.
253 *Supra,* para. 6, preamble DGA.
254 *Supra,* para. 10, preamble DGA and Art. 3(1) DGA.
255 *Supra,* Art. 4 DGA.
256 *Supra,* Art. 5(2) DGA.
257 *Supra,* Art. 3(a) DGA.
258 *Supra,* Art. 6(1) ODD Directive.
259 *Supra,* Art. 6(1), Art. 10 and Art. 14(1)(a) ODD Directive.
260 *Supra,* Art. 6(1) DGA.
261 *Supra,* Art. 6(4) DGA.

3.3. B2G data sharing

Business2Government is the most recent typology of data sharing. In the context of the COVID-19 pandemic, few online platforms voluntarily shared data with public authorities, in order to cope with the health care emergency.[262] In the aftermath of the coronavirus pandemic, the EU Commission has included rules on B2G data sharing in the context of the proposed Data Act. Since the Data Act is still a proposal, this typology of data sharing remains, for the moment, unregulated at the EU level.

Art. 14 of the proposed Data Act provides for a mandated data sharing obligation in the context of "exceptional need": a public sector body may order a data holder to share certain types of data in order "to respond",[263] "prevent" or "assist the recovery" from a "public emergency".[264] The Data Act preamble specifies that a 'public emergency' might be public health related (e.g., forecasting the emergence of new pandemic wave via Big Data analytics), as well emergencies represented by natural disasters and cyber-attacks.[265] Alternatively, a public sector body might ask a data holder to share data in order to fulfil "a specific task in the public interest that has been explicitly provided by law", either in the public authority could not receive the data "by alternative means" (e.g., buying the dataset in the market), or when the data sharing obligation would actually reduce the administrative burden for the data holder.[266]

The proposed Data Act also aims to safeguard data protection, pointing out that the data requested should include, "in so far as possible", non-personal data.[267] Secondly, the data holder should make a "reasonable effort" to anonymize the requested data.[268] However, in a case where the requested data still included personal data, the public authority should process the received data in accordance with GDPR requirements.[269] In any case, the public authority should destroy the data received after the end of the exceptional need that justified the compulsory data sharing.[270]

The requesting authority may share the data received with other public bodies that are also engaged in responding to the public emergency.[271] By contrast, the recipient authority should not share the received data further with other private entities, in accordance with the requirements of the ODD Directive.[272]

In terms of compensation, the data holder shall provide the requested data "free of charge".[273] According to the Data Act preamble, public emergencies are "rare", and thus the business activities of the data holder are not expected to be negatively affected by the data sharing obligation.[274] However, in a case in which data sharing was requested in order to fulfil a "specific task [that is] in the public interest", rather than responding to an exceptional public emergency, the data holder might be entitled to claim compensation.[275] The latter should not exceed the "technical and organizational costs" incurred by the data holder in complying with the data sharing requests, including the costs faced by the data holder in anonymizing the requested data, "plus a reasonable margin."[276] The data holder should inform the public authority about the calculation method of the costs incurred to share the data. and on the criteria used to assess the "reasonable margin."[277]

262 Via the COVID-19 Open Data initiative, for instance, Google shared, free of charge, relevant data concerning the COVID pandemic with scientists and health authorities.
<https://cloud.google.com/blog/products/data-analytics/free-public-datasets-for-covid19> (last accessed 16.8.2022).
263 *Supra,* Art. 15(a) Data Act proposal.
264 *Supra,* Art. 15(b) Data Act proposal.
265 *Supra,* para. 57, preamble to proposed Data Act.
266 *Supra,* Art. 15(c) proposed Data Act.
267 *Supra,* Art. 17(2)(d) proposed Data Act.
268 *Supra,* Art. 18(5) proposed Data Act.
269 *Supra,* Art. 19(1)(b) proposed Data Act.
270 *Supra,* Art. 19(1)(c) proposed Data Act.
271 *Supra,* Art. 17(4) proposed Data Act.
272 *Supra,* Art. 17(3) proposed Data Act.
273 *Supra,* Art. 20(1) proposed Data Act.
274 *Supra,* para. 67, preamble to the proposed Data Act.
275 *Supra,* para. 67, preamble to the proposed Data Act.
276 *Supra,* Art. 20(2) proposed Data Act.
277 *Supra,* Art. 20(2) proposed Data Act.

The meaning of "reasonable margin" is not completely clear. On the one hand, the Data Act's preamble points out that the compensation for the B2G data sharing should not constitute "payment for the data itself".[278] On the other hand, the reference to the reasonable margin implies that that the data holder may make a degree of profit from the data sharing obligation. According to Richter, the data holder should not be entitled to receive only compensation of the marginal costs faced in the contest of data sharing, rather than enjoying a profit margin.[279] Since B2G data sharing should take place in case of purely exceptional circumstances, in fact, the lack of profit would not undermine the data holder's incentives to collect and process the data. Secondly, even if we accepted the idea that the data holder should be entitled to receive some degree of profit, it is worth noticing that the proposed Data Act relies on 'costs + reasonable profit margin' for repeated B2G data sharing, rather than on the FRAND formula. As discussed in the previous sub-section, FRAND is the compensation formula provided by the chapter of the Data Act concerning B2B data portability. It is not fully clear why the draft legislation has opted for two different compensation formulae in relation to B2B and B2G data sharing. In addition,

3.4. Compensation under the EU regulatory framework on data sharing

It could be argued that the determination of the compensation terms and conditions should be left to the agreement of the parties, due to the multiplicity of scenarios that may arise in data sharing. In fact, it would be very difficult to define, *ex-ante,* a compensation mechanism for each data sharing typology.

The EU legal framework does not follow this approach: while leaving to the parties the precise determination of the compensation level, the EU legal framework defines general criteria to determine compensation, both in cases where the data sharing is freely agreed upon by the parties, and when it is mandated by law.

As can be noticed from Figure 2, the EU legal framework refers to 3 main typologies of compensation: 'free access'; a fee based on the marginal costs of data sharing; and Fair, Reasonable and Non-Discriminatory (FRAND) compensation. A fourth typology, which can be defined as 'quasi-FRAND', refers to situations in which the EU legislation demands non-discriminatory and proportional compensation for the data holder; however, the FRAND formula is not fully and properly mentioned in the legislation.

As can be noted from Figure 2, different pieces of EU legislation introduce divergent rules on the compensation level in relation to the same modality of data sharing. Firstly, the ODD and the DGA diverge in relation to the compensation for the data provided by public sector agencies: in fact, while the ODD emphasizes that G2B data sharing should take place free of charge, eventually allowing the public institution to recover of the marginal costs of the documents' disclosure, the DGA opts rather for a costs compensation mechanism.

Secondly, in the context of B2B data sharing, while GDPR and the DMA point out that data portability should take place free of charge, the proposed Data Act stresses that compensation should be FRAND. The rationale followed by the 3 pieces of legislation is different: for the GDPR, the 'free' regime is justified by the fact that data portability is a right of the data subject, while, for the proposed Data Act, the FRAND mechanism compensates for the data holders' efforts in terms of data collection. Finally, the 'free of charge' data portability regime covered in the DMA is justified by the need to tamper with the gatekeepers' market power. However, in relation to the 'blurred' distinction between personal and non-personal data and the overlaps between the different legislations, the compensation regime for data portability remains unclear; potentially generating disputes between data subjects/users and different business users in the future.

278 *Supra,* para. 67, preamble to the proposed Data Act.

279 Heiko Richter, 'Access to Private Sector Data for the Common Good.' CERRE working paper, published in February 2023. The text of the paper is available at: <https://cerre.eu/publications/access-to-private-sector-data-for-the-common-good-a-critical-review-of-chapter-v-of-the-proposed-data-act/> (last accessed 21.3.2023).

Finally, the compensation regime for mandated B2B data sharing is also unclear, and this is where we can find different FRAND variations (i.e., 'quasi-FRAND). Only the DMA, the Motor Vehicles Directive, REACH and the EECC, in fact, openly refer to the FRAND Principle. Taking in consideration this different formula, it remains unclear how the sector-specific rules on mandated B2B data sharing will interact in the future with horizontally applicable rules, especially with the proposed Data Act.

FRAND is a form of data sharing compensation that is often referred to within the EU regulatory framework, especially in terms of data portability and mandated B2B data sharing. However, FRAND is never clearly defined in any EU data sharing legislation. In view of the growing importance of FRAND in B2B data sharing, the next section discusses the meaning of Fair, Reasonable and Non-Discriminatory compensation, by looking at the licensing of Standard Essential Patents (SEPs) and antitrust remedies, in which FRAND is a rather well-accepted principle.

Figure 2: Compensation for different typologies of data sharing under EU law

	Data portability	***Mandated B2B data sharing***	***G2B data sharing***	***B2G data sharing***
GDPR	FREE			
Data Act (draft)	FRAND; COST			FREE: COST
DMA	FREE	FREE; FRAND		
REACH		FRAND		
PSD2		Quasi-FRAND		
Motor Vehicles		FRAND		
Electricity		Quasi-FRAND		
EECC		FRAND		
Postal Services		Quasi-FRAND		
ODD			FREE; COST	
DGA			COST	

FREE: free of charge.

COST: fee based on the marginal costs of data sharing.

FRAND: Fair, Reasonable and Non-Discriminatory terms.

Quasi-FRAND: compensation should be proportionate and non-discriminatory, BUT there is no reference to the actual FRAND formula.

Source: author's own illustration.

4. FRAND in B2B data sharing

4.1. Comparing FRAND under different EU policies

As discussed in Section 3, the emerging EU regulatory framework on data sharing often refers to the principle of FRAND in the context of B2B data sharing. Firstly, under Arts. 8 and 9 of the proposed Data Act, the data holder, following a request from the user, should "make available" to third parties the "data generated by the use of a product" on a non-discriminatory basis and at a reasonable rate (i.e., data portability of non-personal data). Secondly, under Art. 6(11) DMA, search engines that have a gatekeeper status shall provide to competing search engines "ranking, query, click and view data" which are generated by end-users on a FRAND basis. Similarly, under Art. 112(1) EECC, telecoms operators shall share the data concerning telephone numbers and users with the providers of telephone directory enquiry services. (i.e., mandated B2B data sharing). Finally, a few pieces of sector legislation that mandate B2B data sharing include a 'quasi-FRAND' formula: the latter refers to the basic logic of FRAND without mentioning the proper wording of this 'magical' formula.

Art. 10 of the proposed Data Act requires every EU Member State to establish dispute settlement bodies to oversee deciding whether FRAND has been correctly determined in the context of disputes involving the data portability of non-personal data. Art. 13 of the proposed Data Act lists a number of contractual terms that may be considered 'unfair' when imposed by the data holder on a Small and Medium Enterprises (SMEs). On the other hand, the meaning of 'fair' behaviour during the negotiations, 'reasonable' remuneration and 'non-discriminatory' terms are not fully clarified by the proposed Data Act. Similarly, the meaning of FRAND is generally not spelt out in the other legislation concerning B2B data sharing.

As Heim and Nikolic argue, the principle of FRAND appears in legislations across different EU policies, [280] and thus it may be a sort of general principle of EU law. During the past two decades, the principle of FRAND has been extensively interpreted in the context of disputes involving the licensing of Standard Essential Patents (SEPs), within Standard Development Organizations (SDOs), in fact, every SEP holder commits to license its patents to potential licensees on FRAND conditions. The principle of FRAND is also present in EU competition law: in designing antitrust remedies, in fact, the EU Commission and National Competition Authorities (NCAs) often include a FRAND obligation in their decisions under Art. 102 TFEU. In particular, the firm(s) that are subject to the remedies may be required to grant access to their infrastructure/IP/dataset to third parties (often competitors) under FRAND terms.[281] Similarly, FRAND access remedies have been included by the EU Commission in its merger decisions in different industries, e.g., medical equipment, television broadcasting, payment processing, gas networks, flight search, missile systems, technology platforms and herbicides.[282] The FRAND principle thus goes beyond standard essential patents; it is a key-feature of the access remedies adopted by the EU Commission, both under Art. 102 TFEU and in merger control.

Both in SEPs licensing and in competition law remedies, the principle of FRAND aims to promote 'access' to a key technology/infrastructure. In particular, FRAND aims to 'cure' the perceived negotiation imbalance between the IP/asset's holder and those third parties that would like to have access to the facility. FRAND may thus be considered a pre-contractual commitment[283] which limits the freedom of the patent holder/firm subject to the antitrust remedies. On the other hand, FRAND also safeguards the interests of the IP/asset's holder: by requiring 'reasonable' compensation, in fact, FRAND recognizes that the asset's holder should be compensated for the efforts/investments that it had previously carried out to develop and maintain the facility, which has now acquired the position of playing a critical role for those third parties. In other words, a zero-license rate may hardly

280 Mathew Heim, Igor Nikolic (2019), "A FRAND Regime for Dominant Digital Platforms." 10(1) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law:* 19.

281 Frank Maier-Rigaud, Benjamin Loertscher (2020), 'Structural vs. behavioural remedies.' *Competition Policy International.* The paper is available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3569642> (last accessed 27.1.2023), p.4.

282 *Supra,* Heim and Nikolic, p. 19.

283 Igor Nikolic, *Licensing Standard Essential Patents: FRAND and the Internet of Things* (Bloomsbury Publishing, 2021), p. 85.

be considered compatible with the FRAND principle.

B2B data sharing takes place in accordance with a license agreement between the data holder and the potential data recipient; such an agreement defines the terms and conditions of data access/re-use, as well as potential compensation. A B2B data sharing agreement thus shares similarities with a SEP license agreement.[284] As discussed in Section 2, B2B data sharing is currently undermined by a number of market failures; the negotiation imbalance between the parties may encourage the data holder either to refuse to conclude a license agreement, or to impose unfair terms and conditions on the potential data recipient. Similarly to SEPs and competition law remedies, the principle of FRAND, in the context of B2B data sharing, thus aims to solve such a negotiation imbalance by defining general conditions for the data sharing negotiations. Finally, by not determining, *ex-ante,* a precise compensation rate, the FRAND principle also safeguards the efforts of the data holder in collecting and processing the data that are included in the dataset.

The FRAND principle in competition law remedies, SEPs licensing and B2B data sharing are also characterized by relevant differences. Firstly, while a FRAND commitment in SEPs licensing is an example of 'self-regulation' that aims to prevent a market failure, in competition law remedies, by contrast, the FRAND principle is imposed by a competition authority and it aims to solve, rather than to prevent, the negotiation imbalance discussed above. Secondly, the SEP holder/firm who is subject to competition law remedies 'owns' a patent right/essential asset. By contrast, in the context of B2B data sharing, the data holder 'controls' the dataset, but does not have a legal ownership right over the dataset.[285] Thirdly, while, in the context of SEP licensing and competition access remedies, the third party would pay a royalty fee to the asset's holder, compensation in B2B data sharing often has a non-monetary nature, and. as discussed in Section 2, the recipient might provide data analytics services to the data holder, rather than paying monetary compensation. Finally, unlike SEP licensing and competition access remedies, the relationship between the data holder and the recipient is often mediated by an intermediary.

While these differences should be born in mind, it is worth comparing the application of the principle of FRAND in the three policy areas. It is worth interpreting the meaning of FRAND in B2B data sharing, in the light of the lessons learnt in SEP licensing and in competition law remedies. In this regard, the next sections discuss the meaning of 'fair' behaviour during the negotiations, 'reasonable' compensation, and 'non-discriminatory' conditions in SEPs licensing, competition law remedies and B2B data sharing.

284 *Supra,* Picht (2022), p. 8.
285 *Supra,* Richter, Slowinski (2019), p. 21.

4.2. 'Fair' behaviour during the license negotiations

4.2.a. 'Fair' behaviour in SEPs licensing negotiations

In its landmark ruling in *Huawei v. ZTE,*[286] the EU Court of Justice provided useful guidelines on how the parties should behave 'fairly' during SEP licensing negotiations. It is thus worth briefly summarizing the ruling*,* as well as the follow-up judgments by the German courts that have further clarified the meaning of the negotiation steps identified by the CJEU in *Huawei v. ZTE.*

The case concerns a license dispute between two Chinese manufacturers of mobile phone equipment. On the one hand, Huawei held several patents that were 'essential' for the development of the 4G mobile phone standard. In the context of the standardization process carried out by the European Telecommunications Standards Institute (ETSI), Huawei committed to license its SEPs on FRAND terms.[287] On the other hand, ZTE was an implementer – i.e., a manufacturer of mobile phones, that relied on the 4G standard. Though ZTE had shown an initial interest in licensing Huawei's patents portfolio, the parties could not agree on a FRAND license rate.[288] With the lack of an agreement, Huawei requested that the Düsseldorf District Court issue an injunction prohibiting ZTE from selling its products that relied on Huawei's SEPs in the German market.[289] The Düsseldorf District Court referred five preliminary ruling questions to the Court of Luxembourg: the national court essentially asked the EU Court of Justice whether, and to what extent, a request for a court injunction by a SEP holder might represent an abuse of dominance, in breach of Art. 102 TFEU.[290]

In line with the questions submitted by the Düsseldorf District Court, the CJEU ruled that the SEP holder could legitimately ask for a court injunction, without breaching Art. 102 TFEU, only if the implementer did not comply with the negotiation steps identified by the CJEU in its preliminary ruling.[291] In other words, the SEP holder could ask for a court injunction only if the implementer did not behave in a 'fair' manner during the negotiations, and thus it could not be considered a 'willing licensee' – i.e., it could not benefit from the FRAND commitment offered by the SEP holder in the context of the standardization process. Rather than having a general discussion on the meaning of FRAND, therefore, in *Huawei v. ZTE, the Court of Justice defined a FRAND-based framework that the SEP holder and the potential licensee should follow during the negotiations.*

According to the EU Court of Justice, as a first step, the SEP holder should notify the implementer that, by marketing products covered by its patents, it had breached its patent rights.[292] According to the EU Court of Justice, taking into consideration the large number of patents that fall within the scope of an industry standard, it could not be presumed that the implementer had voluntarily breached the SEP holder's patent rights – i.e., the implementer was not aware of the patents breached by releasing products onto the market that implemented the industry standard.[293] From this perspective, the prior infringement notification aimed to clarify whether the implementer was truly willing to license the SEPs. In the follow up to *Huawei v. ZTE,* the German courts have clarified the scope of the notification obligation.[294] The SEP holder had to specify which patent(s) had been infringed, inform the other party that the patent(s) had been declared standard-essential, indicate the name of the relevant standard, and point out which functionalities of the products manufactured by the third party breached the patent(s). The UK Court of Appeal pointed out, in *Unwired Planet,* that the notification was a mandatory condition that the SEP holder should always satisfy before asking for a court injunction.[295] However, the precise content of such a notification might vary, depending on

286 Case C-170/13, *Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH* (2015) ECLI:EU:C:2015:477.
287 *Ibid,* para. 24.
288 *Ibid,* para. 26.
289 *Ibid,* para. 27.
290 *Ibid,* para. 39.
291 *Ibid,* para. 58.
292 *Ibid,* para. 61.
293 *Ibid,* para. 62.
294 *NTT DoCoMo v HTC*, Regional Court (Landgericht) of Mannheim 29 January 2016 - Case No. 7 O 66/15.
295 Court of Appeal of England and Wales, *Unwired Planet v. Huawei,* 23 October 2018. [2018] EWCA Civ 2344.

the specific circumstances of each case.[296]

As a second step, the implementer should reply to the initial notification and inform the SEP holder about its intention to engage in negotiations, with a view to concluding a license agreement.[297] The German courts have pointed out that, in their reply to the initial notification, the implementer should express, unambiguously, its willingness to engage in negotiations in order to conclude a licence agreement.[298] Secondly, the implementer should not engage in delay tactics when replying to the initial notification. In particular, in *Saint Lawrence v Vodafone,* the Düsseldorf Regional Court pointed out that the more detailed the initial infringement notification is, the less time the implementer has to reply to the SEP holder.[299] The SEP holder could thus ask for a court injunction only in a case where the implementer did not reply to the infringement notification, or if it excessively delayed its reply, in order to avoid the start of the licensing negotiations.

As a third step, the SEP holder should make a license offer on FRAND terms.[300] In *Pioneer v Acer*, Mannheim Regional Court stressed that the offer should contain all of the essential contractual terms needed to enable the parties to directly conclude a licensing agreement: in the case that the implementer accepted the initial offer, the agreement should rely on the terms indicated by the SEP holder's initial offer.[301] In particular, the offer should include a method to calculate a 'reasonable' license rate, so that the implementer could verify whether the requested fee is indeed FRAND.[302]

The implementer could either accept the initial offer from the SEP holder or make a counter proposal.[303] In *Sisvel v. Haier, the Düsseldorf Regional Court pointed out that the implementer should always reply to the initial license offer, even if the latter was not considered FRAND.*[304] The implementer counteroffer should also be compliant with the FRAND principle.[305] Similarly to the previous steps, in a case in which the implementer refused to cooperate (e.g., by not making any counter-offer), the SEP holder could legitimately ask for a court injunction.

Finally, it would be up to the SEP holder to either accept or reject the counteroffer. In the latter case, the implementer should provide sufficient security to show that it would have adequate financial resources to conclude a license agreement. According to the CJEU, the implementer can either provide a bank guarantee or offer proof of having transferred a certain sum of money to a bank deposit.[306] In *Sisvel v Haier, the Düsseldorf District Court pointed out that the security offered by the implementer should be sufficient to cover the license rate mentioned in the implementer's counteroffer.*[307] Secondly, the fact that the implementer would stop selling the products that breached the patents that are the object of the dispute would not eliminate its duty to offer proper securities.[308] Finally, with the lack of an agreement, the parties could refer the matter to "an independent third party" (i.e., an arbitral tribunal or a national court), which would decide on the appropriate FRAND license rate.[309]

296 *Ibid.*
297 *Supra,* Case C-170/13, para. 63.
298 See, for instance:
VoiceAge v HMD, Regional Court (Landgericht) of Munich, 19 August 2021 - Case No. 7 O 15350/19.
LG v TCL, District Court (Landgericht) of Mannheim, 2 March 2021 - Case No. 2 O 131/19.
Conversant v Daimler, Regional Court (Landgericht) of Munich I, 30 October 2020 - Case No. 21 O 11384/19.
299 *Saint Lawrence v Vodafone*, Regional Court (Landgericht) of Düsseldorf, 31 March 2016 - Case No. 4a O 73/14
300 *Supra,* Case C-170/13, para. 63-64.
301 *Pioneer v Acer*, Regional Court (Landgericht) Mannheim, 8 January 2016 - Case No. 7 O 96/14.
302 *Philips v Archos*, Regional Court (Landgericht) of Mannheim, 17 November 2016 - Case No. 7 O 19/16.
303 *Supra,* Case C-170/13, para. 66.
304 *Sisvel v Haier*, Regional Court (Landgericht) of Düsseldorf, 3 November 2015 - Case No. 4a O 144/14.
305 *Saint Lawrence v Deutsche Telekom*, Regional Court (Landgericht) of Manheim, 27 November 2015 - Case No. 2 O 106/14.
306 *Supra,* Case C-170/13, para. 67.
307 *Sisvel v Haier*, Regional Court (Landgericht) of Düsseldorf, 3 November 2015 - Case No. 4a O 93/14.
308 *Pioneer v Acer*, Regional Court (Landgericht) Mannheim. 8 January 2016 - Case No. 7 O 96/14
309 *Supra,* Case C-170/13, para. 68.

4.2.b. 'Fair' license negotiations in EU competition law remedies

In its Decisions, the EU Commission has often emphasized that the firm(s) subject to remedies should provide access to their assets, 'without delay', to any interested third party.[310] Secondly, in its 2004 Decision, the EU Commission requested that Microsoft provide interoperability information to competing software manufacturers only after it had a "working and sufficiently stable implementation" of its new work group server operating system.[311] In other words, the data access obligation was applicable only from the moment Microsoft had completed the trial phase of its new operating system. This solution would avoid competitors making any useless investment in making their software compatible with a prototype operating system that Microsoft would later not release in the market. Similarly, the EU Commission also pointed out that "terms imposed by Microsoft in the future should be sufficiently predictable."[312] In other words, Microsoft would not be able to modify the license conditions of its interoperability information unilaterally. Such unilateral change, in fact, would harm the investments carried out by third parties to make their software compatible with Microsoft's operating system.

The requirements mentioned clarify how the firms that are subject to remedies should grant 'fair' access to their assets to third parties. However, these indications are quite generic, and they only refer to the behaviour of the firm(s) that are subject to remedies. In other words, in its antitrust and merger Decisions, the EU Commission has never provided a detailed 'fair' negotiation framework which is comparable to that elaborated by the CJEU in *Huawei v. ZTE.* For instance, while the EU Commission has pointed out that the firm(s) that are subject to remedies should provide access 'without delay', as soon as the product trial phase is completed, the EU Commission has not clarified whether the third parties should be required to accept the initial offer, or whether they can submit a counteroffer.

Finally, it is worth bearing in mind that the implementation of the access remedies is usually supervised by a Monitoring Trustee – i.e., an independent third party appointed by the EU Commission to supervise the implementation of the remedies. In particular, the monitoring trustee would try to mediate between the parties in the case of a disagreement on the implementation of the EU Commission's access remedies. Secondly, the monitoring trustee would periodically report to the EU Commission about the status of implementation of the remedies. The EU Commission, for instance, appointed a Trustee to check that Microsoft granted access to the necessary interoperability information to its competitors.[313] The EU General Court, however, quashed the section of the Commission Decision which required Microsoft to bear the entire cost entailed by the Monitoring Trustee.[314] In light of the General Court's ruling, and the changes in Microsoft's behaviour, in 2009, the Commission decided to no longer appoint a full-time monitoring trustee to assess Microsoft's compliance, opting for the *ad hoc* assistance of technical consultants.[315] Although the Monitoring Trustee was not a successful solution in the *Microsoft* case*,* the latter may be considered an attempt to avoid the referral of the dispute to a court/arbitration, and it thus represents a further difference in comparison to the *Huawei v. ZTE* negotiation scheme, which does not provide for such a solution.

310 Commission Decision of 30 April 2003 declaring a merger to be compatible with the common market and the EEA Agreement (Case COMP/M.2861— Siemens/ Drägerwerk/ JV). Para. 156.

311 Commission Decision of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation. OJ L-32/23, 6.2.2007. Para. 1009.

312 *Ibid,* para. 1008(IV).

313 Commission Decision of 28.07.2005, relating to a proceeding under Art. 82 of the Treaty (Case Comp C-3/37.792, *Microsoft*).

314 Case T-201/04, *Microsoft v. Commission* (2007) ECLI:EU:T:2007:289.

315 Commission Decision of 4.3.2009 on the deletion of Art. 7 of Decision 2007/53/EC relating to a proceeding pursuant to Art. 82 of the EC Treaty and Art. 54 of the EEA Agreement against Microsoft Corporation and repealing Decision C(2005)2988 final (Case COMP/37.792 – *Microsoft*).

4.2.c. 'Fair' behaviour during the data sharing negotiations

The basic question discussed in this sub-section is whether, and to what extent, the lessons drawn from SEP licensing and EU competition access remedies on the 'fair' behaviour that the parties should keep during the negotiations might be applicable in the context of B2B data sharing.

According to Drexl, an important difference between SEP licensing and B2B data sharing should be borne in mind:[316] while an industry standard is publicly available, and thus the implementer can start releasing the products that implement the standard before concluding a licensing agreement with the SEP holder, in B2B data sharing the potential recipient is not aware of the content of the dataset. In other words, while a patent infringement is the starting point of every SEP licensing negotiation, in the context of B2B data sharing, it is very unlikely that the recipient will get access to the dataset where there is the lack of a sharing agreement.

Secondly, as discussed in Section 2, it is worth bearing in mind that B2B data sharing is often characterized by non-monetary remuneration. While, in the context of SEP licensing, the implementer usually agrees to pay a royalty rate to the patent holder, in B2B data sharing, the recipient may remunerate the data holder by providing specific data analytics services. In addition, while SEP licensing implies a direct agreement between the patent holder and the implementer, in B2B data sharing the relationship between the parties is often mediated by an intermediary.

The *Huawei v. ZTE* negotiation framework should therefore be adjusted in view of the specific features of B2B data sharing. First, while in SEP licensing it is always the patent holder who has to contact the implementer via the infringement notification, in B2B data sharing it would be up to the potential recipient to contact the data holder, expressing their wish to conclude an access agreement. Since the potential recipient would be unaware of the precise content/quality of the dataset, it would not be able to express an initial FRAND offer. By contrast, after having received the initial request notification, the data holder could submit a FRAND-based offer. In other words, in the context of B2B data sharing, the negotiation process would be started, generally, by the potential data recipient, rather than by the data holder. The access request would replace the patent infringement notification in the context of the *Huawei v. ZTE* negotiation framework.

This clarification is rather important in the context of the EU legislations on mandated data sharing. Art. 6(11) DMA, for instance, points out that the gatekeeper "shall provide" access to "ranking, query, click and view data" at the request of competing online search engines. By contrast, the Motor Vehicles Regulation, Electricity Directive, EECC and REACH do not clearly point out whether the potential recipient should submit an access request to the data holder. In the context of data portability, the access request should originate from the data subject/user. As pointed out by Art. 5(1) of the proposed Data Act, the data holder should grant access to the dataset "upon request by the user". Since the dataset includes data generated by the user during the product use, it would be up to the individual user to inform the data holder about their wish to share the data generated with third parties. From this perspective, Art. 5(1) of the proposed Data Act mirrors Art. 20(2) GDPR, which provides that the data user should ask the controller to transmit his/her personal data to a third party. Neither the GDPR nor the Data Act proposal, however, clarify whether the user/data subject can express a general authorization to allow the data holder/controller to share the data with a third party, or whether the user/data subject should provide a single authorization every time that the data is transferred to the third party.

316 Josef Drexl et al. (2022), *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act).* Para. 102. The document is available at: <https://pure.mpg.de/pubman/faces/ViewItemOverviewPage.jsp?itemId=item_3388757> (last accessed 2.2.2023).

While the peculiarities of B2B data sharing make it difficult to apply the first two steps of the *Huawei v. ZTE* negotiation framework, the following steps could be applied, *mutatis mutandis,* in the case of B2B data sharing. First, in line with the case law developed by the German courts, the license offer should be 'completed' – i.e., it should contain all the essential contractual terms to enable the parties to directly conclude a licensing agreement in a case where the potential recipient has accepted the proposed conditions.[317] In particular, the data holder could include in the offer a calculation method, in order to clarify for the potential recipient why the offer is FRAND-based.[318] This requirement has now been codified in the proposed Data Act under Art. 9(4), in fact, the data holder:

> "… shall provide the data recipient with information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can verify…" whether the offer is indeed FRAND basis.

In addition, considering the lessons drawn from competition law access remedies, we might argue that the data holder should provide the offer 'without delay'.[319] In addition, the conditions proposed by the data holder should be 'stable':[320] the data holder cannot change the conditions unilaterally in the future, in order to safeguard the investments previously made by the recipient during the use of the dataset.

As in *Huawei v. ZTE*, in the case that the potential recipient rejects the data holder's initial offer, it would be required to submit a FRAND-based counteroffer. Finally, in a case where the data holder rejects the counteroffer, the recipient could be required either to provide a bank guarantee or a bank deposit, with a value that is at least equivalent to the proposed counteroffer.[321]

Finally, the parties can refer any dispute to an independent body. In this regard, it is worth bearing in mind that the Data Act proposal requires the EU Member States to establish specific dispute settlement bodies, which have the jurisdiction to decide on disputes between the data holder and the recipient.[322] Once established, these bodies should take into consideration the *Huawei v. ZTE* ruling, in order to decide whether, and to what extent, the parties did indeed behave 'fairly' during the negotiations.

Overall, except for the first two steps, the *Huawei v. ZTE* negotiation framework could be applied, mutatis mutandis, in the context of B2B data sharing. Nevertheless, the framework should be adjusted, on a case-by-case basis, according to the different typologies of B2B data sharing. In particular, the framework could still be applicable in a case in which the remuneration included those data analytics services that are provided by the recipient to the data holder. The data holder's offer, in fact, could indicate this type of remuneration. By contrast, the presence of an intermediary in the relationship between the data holder and the recipient would make the *Huawei v. ZTE* negotiation framework barely applicable.

317 *Supra,* Case No. 7 O 96/14.
318 *Supra,* Case No. 7 O 19/16.
319 *Supra,* Case COMP/M.2861.
320 *Supra,* Commission Decision in *Microsoft.*
321 *Supra,* Case No. 4a O 93/14.
322 *Supra,* Art. 10 Data Act proposal.

4.3 'Reasonable' license rate

4.3.a. 'Reasonable' license rate of SEPs

During the past two decades, US courts have engaged in the estimation of a 'reasonable' royalty rate when ruling on damages claims involving a breach of Standard Essential Patents.[323] In such a context, economists, who are hired as experts by the parties, and/or by the tribunal, have elaborated a number of methods through the use of which to estimate what a 'reasonable' license rate should look like.

Firstly, several economists have supported the so-called '*ex-ante* incremental value approach': a 'reasonable' license rate should include only the value of the licensed technology before the standard was adopted within the SDO, and thus the patent became 'essential'.[324] Economists who support the *ex-ante* approach have elaborated different methods with which to implement this approach in concrete terms. In particular, Lerner and Tirole have argued that the SEP holder should voluntarily commit to a price cap in relation to the maximum royalty rate that it will demand from potential licensees.[325] This value may be determined by assessing the incremental value of the patent(s) selected as a standard, in comparison with the best alternative technology available at the time that the standard was adopted. Alternatively, Swanson and Baumol have elaborated an auction model, where every patent holder would put up for auction its SEPs, within the SDO at the time when the standard is adopted.[326] Neither the royalty cap nor the auction model, however, have ever been implemented in practice. On the one hand, SSOs have always refused to become involved in the assessment of FRAND terms in relation to specific SEPs, leaving the definition of what a "reasonable" royalty rate is to the bilateral negotiations between their members. On the other hand, the auction model is difficult to implement in practice, since, at the time when the standard is adopted it is still unclear what the future profit margin of the component produced on the basis of the SEPs will be, and the margin that might provide an indication of the minimum royalty rate that the SEP holder can demand in the context of an hypothetical auction.[327] Similarly, Nikolic has argued that the *ex-ante* approach is not in line with the way in which the standardization process takes place within an SDO. *Ex ante* methods, in fact, generally take for granted that multiple technologies had 'competed' to be selected by the SDO as the industry standard. In reality, SDOs 'develop' a standard over a long period of time via a joint effort by the industry players (i.e., the implementers and the SEP holders). It is thus very difficult (almost impossible) to identify competing technologies, and their corresponding values, before the standard has been adopted.

323 See, in particular:
- *Microsoft v. Motorola,* 2013 WL 2111217 (WD Wash 2013).
- *In re Innovatio IP Ventures,* 2013 WL 5593609 (ND Ill. 2013).
- *Apple v. Motorola,* 869 F. Supp. 2d. 901, 913 (ND Ill 2012).
- *Ericsson v D-Link 773 F.3d 1201 (Fed Cir 2014).*
- *CSIRO v Cisco*, 2015 WL 7783669 (Fed Cir 2015).
- *TCL v Ericsson*, 2017 WL 6611635 (CD Cal 2017).

324 Among the supporters of this approach, please see:
- Daniel Swanson, William Baumol (2005), 'Reasonable and Non-discriminatory (RAND) Royalties, Standards Selection, and Control Market Power' 73 *Antitrust Law Journal:* 1.
- Mark Lemley, Carl Shapiro (2007), 'Patent Holdup and Royalty Stacking' 85 *Texas Law Review:* 2040.
- Joseph Farrell et al. (2007), 'Standard Setting, Patents and Hold-up' 74 *Antitrust Law Journal:* 603.

325 Josh Lerner, Jean Tirole (2015). 'Standard-Essential Patents'. 123(3) *Journal of Political Economy*: 547.

326 *Supra,* Swanson and Baumol.

327 Damien Geradin, Anne Layne-Farrar and A. Jorge Padilla (2008), 'Competing Away Market Power? An Economic Assessment of *Ex Ante* Auctions in Standard Setting' 4(2) *European Competition Journal:* 443.

Some economists have proposed alternative *ex-ante* models, in which the royalty rate is assessed, not at the time when the standard is agreed upon within the SDO but, rather, in the context of a hypothetical negotiation between the SEP holder and the potential licensee taking place where there is the lack of judicial litigation. The main method that follows the *ex-ante* hypothetical logic is the 'top-down' approach.[328] The latter method firstly requires the establishment of a cumulative royalty rate for the entire standard, and then the calculation of the share of individual SEPs within the total royalty rate.[329] Confidentiality clauses, which usually bind the SEPs holders in relation to license conditions that have previously been agreed with other licensees, may represent an obstacle to the application of the top-down approach.[330] The lack of transparency in the SEPs negotiations, in fact, undermines the possibility of assessing the total value of the standard and then dividing it by the applicable patents that are considered to be essential for its implementation. Secondly, the question is how royalties can be distributed among the different SEP owners that have contributed to the same standard.[331] Some authors have argued that a numeric proportionality approach would represent an easy rule of thumb to apply: every patent considered essential for the standard implementation should be remunerated in accordance with a standard royalty basis.[332] Nevertheless, the numeric proportionality approach fails to take into consideration the "contribution" that each SEP has made in relation to the implementation of the standard.[333] In particular, SEP holders often tend to "over-declare" the "essentiality" of their patents to the implementation of the standard; the numeric proportionality approach thus incentivizes the phenomenon of SEP over-declaration.[334]

An alternative, more practiced-oriented, approach is based on the assessment of 'comparable' license rates, such as the rates requested by the SEP holder from other licensees in the context of previous negotiations. Previous license rates thus become a sort of 'benchmark' against which to assess how 'reasonable' the requested rate is. The logic behind this method is that if a license rate has been previously accepted by other licensees (i.e., it was not challenged in Court as being non-FRAND based) it should be 'reasonable'.[335] The benchmarking approach also has some shortcomings, which form an obstacle to its application. Firstly, the question is to identify 'comparable' licenses. As noted by Nikolic, licenses should not be compared only on the basis of the requested royalty rate, but also on the basis of their terms and conditions (e.g., geographic scope of application, duration, cross-licensing conditions).[336] In particular, the benchmarking approach is difficult to implement in the case of portfolios of patents: parties, in fact, usually negotiate license agreements covering portfolios of different SEPs that fall within the same standard; every portfolio of licensed patents may differ, so it can cause the scope of the license agreement to differ.[337] Secondly, and similarly to the top-down approach, confidentiality obligations may make it impossible for the SEP holder to disclose the precise content of previous license agreements, thus undermining the application of the benchmarking method. In order to solve this issue, a number of authors have suggested that SDOs should require all patent holders to disclose their SEPs when the standard is adopted.[338] The disclosure of SEPs would make the value of the royalty rate agreed by SEP holders and different licensees more transparent, avoiding the risk of non-discrimination and facilitating the application of both the top-down and the benchmarking approaches in order to achieve a mutually-agreed 'reasonable' license rate.

328 Stefano Barazza (2014), 'Licensing Standard Essential Patents, Part One: the Definition of F/RAND Commitments and the Determination of Royalty Rates' 9(6) *Journal of Intellectual Property Law and Practice:* 472.
329 *Ibid,* Barazza, p. 481.
330 *Supra,* Nikolic, p. 111.
331 *Supra,* Nikolic, p. 112.
332 See, for instance, Anne Layne-Farrar, Jorge Padilla, Richard Schmalensee (2007), 'Pricing Patents for Licensing in Standard Setting Organizations: Making Sense of FRAND Commitments.' CEMFI Working Paper 0702. The working paper is available at: <https://ideas.repec.org/p/cmf/wpaper/wp2007_0702.html> (16.1.2022).
333 *Supra,* Barazza, p. 472.
334 *Ibid.*
335 *Supra,* Nikolic, p. 103.
336 *Supra,* Nikolic, p. 105.
337 *Supra,* Barazza, p. 475.
338 See, for instance, Jorge Contreras (2013), "Technical Standards and *Ex Ante* Disclosure: Results and Analysis of an Empirical Study" 53(1) *Jurimetrics*: 163.

Finally, the 'present value-added' and 'hedonic pricing' are new methods (still not applied by any US Court) that have recently been proposed by a number of economists. Both methods rely on observable market factors to determine whether, and to what extent, the requested license rate is indeed 'reasonable'. In particular, the first method takes into consideration the future cash flows that are expected from the patent licenses, which are then discounted back at an appropriate discount rate in order to determine the technology value before the standard's definition.[339] On the other hand, hedonic price analysis departs from the current market price of a multicomponent product, and, later, determines the value of each component by looking at the willingness of consumers to pay for different components.[340] Both methods are implemented via customer surveys, which aim to identify the consumers' willingness to pay for the technology, and thus to estimate a reasonable value for the SEP.[341]

The top-down and the benchmarking approaches represent the most common methods relied upon by US Courts in order to estimate when a SEP royalty rate may be considered "reasonable".[342] *Unwired Planet*, which was decided upon by the High Court of England and Wales in 2017, represents one of the few cases that hav been decided upon so far in Europein which the tribunal had to decide on the 'reasonable' royalty rate in a SEP-related dispute.[343] After rejecting the royalty estimations put forward by the parties to the case, the High Court favored the benchmark over the top-down approach.[344] However, the High Court stressed that, due to the hypothetical nature of the royalty calculation, the parties should verify their estimations using different methods.[345] Nevertheless, *Unwired Planet* represents an exception in Europe: in line with the *Huawei* ruling by the EU Court of Justice,[346] FRAND has been interpreted by most of national courts of European countries as a negotiation framework.[347] Within such a framework, a 'range' of license rates agreed by the parties may be considered 'reasonable', and thus compatible with the FRAND obligation.[348]

4.3.b. 'Reasonable' license rate in EU competition law remedies

In its Decision in *Liberty Global,* the EU Commission required the merging parties to license TV distributors in Belgium to access the channels Vier and Vijf on a FRAND basis.[349] The Decision relied on the benchmark approach to determine what a 'reasonable' rate should look like. The EU Commission, in fact, concluded that the FRAND rate was represented by the tariff previously asked for by Telenet (i.e., one of the merging parties) to other TV distributors.[350] The rate and quality of the signal provided before the merger by Telenet with third TV distributors was thus considered the appropriate benchmark against which to assess whether, and to what extent, the merging parties had licensed the two TV channels on a FRAND basis.

339 Roya Ghafele, Jan Schmitz (2020), 'Economic Perspectives on FRAND' 11, *Journal of European Competition Law & Practice:* 90.

340 Heins Goddar, Ulrich Moser, 'Traditional Valuation Methods: Cost, Market and Income Approach.' In Federico Munari and Raffaele Oriani (eds), *Economic Valuation of Patents: Methods and Applications* (Edward Elgar, 2011).

341 *Supra,* Nikolic, p. 121.

342 Haris Tsilikas (2020), 'Emerging Patterns in the Judicial Determination of FRAND Rates: Comparable Agreements and the Top-Down Approach for FRAND Royalties Determination.' 69(9) *GRUR International:* 885-892. At 886.

343 High Court of England and Wales, *Unwired Planet International v. Huawei Technologies* [2017] EWHC 711 (Pat).

For a detailed analysis of the High Court ruling in *Unwired Planet,* see Peter Picht (2017), 'Unwired Planet v. Huawei: a Seminal SEP/FRAND Decision from the UK.' Max Planck Institute for Innovation and Competition Research Paper No 17-07.

344 "This approach, in which a rate is determined as a benchmark and then adjustments made as appropriate, is a useful way of determining what a FRAND rate or rates should be."

Ibid, para. 176.

345 Damien Neven, Pierre Régibeau (2017), "Unwired Planet v. Huawei: A Welcome Clarification of the Concept of FRAND and of the Role of Competition Law towards SEP Licensing." 8(7) *Journal of European Competition Law and Practice:* 464.

346 *Supra,* Case C-170/13.

347 Giuseppe Colangelo, Gianluca Scaramuzzino (2019), "Unwired Planet Act 2: the Return of the FRAND Range." 40(7) *European Competition Law Review:* 306.

348 Both the Court of England and Wales in *Unwired Planet,* and the *Bundesgerichtshof* in *Sisvel v. Haier,* have concluded that a 'range' of royalty rates may be considered 'reasonable', and thus compatible, with the FRAND commitment by the SEP holder.

Supra, EWCA Civ 2344. Para. 121.

Bundesgerichtshof, *Sisvel v. Haier*, ruled on 5.5.2020, ECLI: DE: BGH: 2020: 050520UKZR36.17.0 Para. 81.

349 Commission Decision of 24 February 2015, declaring a concentration to be compatible with the internal market and the EEA Agreement (Case M.7194 – LIBERTY GLOBAL/CORELIO/W&W/DE VIJVER MEDIA). C(2015) 996 final.

350 *Ibid,* para. 625.

Except for *Liberty Global,* the EU Commission has generally not relied on the methods discussed in the previous pages in order to define what a 'reasonable' license should look like in its antitrust Decisions. Rather, the EU Commission left it to the parties to negotiate the license rate bilaterally, subject to the possibility of referring an eventual dispute either to a national court or to arbitration. However, in a few decisions, the EU Commission has provided some indications of how a 'reasonable' license rate should be estimated. In its 2004 Decision, the EU Commission forced *Microsoft* to disclose protocol information to its competitors on a FRAND basis, in order to ensure the interoperability among Microsoft work group servers and products that were developed by its competitors.**351** In its Decision, the EU Commission pointed out that the remuneration should not reflect the "strategic value stemming from Microsoft's market power" in the client PC operating system market, nor in the work group server operating system market.[352] Due to its strong market power at that time, Microsoft was the pricemaker in the market. A 'reasonable' license rate, therefore, should be 'lower' than the license rate otherwise requested by Microsoft under ordinary market conditions. While clear in theory, in practice, it would be quite difficult to determine Microsoft's 'strategic value' in the market, and to discount it from the possible license rate.

More recently, in the *Insurance Ireland* commitment decision, the parties committed to revise their fees scheme to grant access to the Insurance Link database.[353] The fee structure should be "fair, objective, transparent and non-discriminatory" for every user. A reasonable access fee should take into consideration 3 parameters:[354] the actual cost incurred by Insurance Link to manage and keep updated the database; the user "actual use" of the database during a specific period of time; an initial fee would be charged on every new user, to cover the fixed costs of setting up the database.

In other Decisions, the EU Commission has introduced further criteria to clarify the meaning of 'reasonable' rate. In *Rambus,* for instance, the firm committed to licensing its patents that were essential for the implementation of the DRAM memory standard for any willing licensee on FRAND terms.[355] The Commission Decision required Rambus to comply with a royalty cap: the maximum worldwide royalty rate requested by Rambus could vary between 1% and 2.65% of the price of the end-user product, depending on the type of device in which the DRAM memory was implemented.[356] In addition, Rambus should follow a most-favored licensee approach: any additional licensee should benefit from the lower royalty rate previously agreed by Rambus with a third party to license the SEPs that fell under the DRAM memory standard.[357]

Rambus is a rather exceptional case: the EU Commission rarely sets a maximum royalty rate in its antitrust Decisions. However, on a few occasions, the EU Commission has emphasized that 'reasonable' compensation should take into consideration only the marginal costs faced by the firm, subject to remedies to grant access to third parties. In *Siemens /Drägerwerk*, for instance, the EU Commission required the newly established joint venture to disclose all information concerning interfaces and communication protocols to third parties on a FRAND basis.[358] In the Decision, the EU Commission ruled that the merging parties should provide the information either free of charge, or eventually cover the documentation costs faced, in order to provide interoperability information to third parties.[359] Similarly, in *Newscorp/Telepiù,* the merging parties committed to granting access to their APIs on a FRAND basis, so that competing pay-TVs could develop interactive services that were compatible with the decoders that were being relied upon by the merging parties.[360] The EU

351 *Supra*, EU Commission Decision in *Microsoft.*
352 *Supra,* EU Commission Decision in *Microsoft*, para. 1008.
353 Commission Decision of 30.6.2022 relating to a proceeding under Article 101 of the Treaty on the Functioning of the European Union (TFEU) and Article 53 of the EEA Agreement Case AT.40511 - *Insurance Ireland: Insurance claims database and conditions of access*. Para. 61(b).
354 *Ibid,* para. 61(b).
355 Commission Decision of 9.12.2009 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case COMP/38.636 – *RAMBUS*).
356 *Ibid,* Annex, on commitments, para. 49(a).
357 *Ibid,* Annex, on commitments, para. 49(e).
358 Supra, Case COMP/M.2861.
359 *Supra,* Case COMP/M.2861. Para. 156.
360 Commission Decision of 02.04.2003 declaring a concentration to be compatible with the common market and the EEA Agreement

Commission Decision pointed out that the license rate should be calculated on a cost-oriented basis, including the long-run incremental costs faced by the merging parties in developing new decoders.[361]

To sum up, in its antitrust and merger Decisions involving access commitments, the EU Commission has often requested that the firms grant access to its facility on FRAND terms. Rather than estimating what is a 'reasonable' license rate, the EU Commission has provided some general guidelines. In particular, the rate should be cost-oriented, including those investments costs faced by the assets' holder. The rate should not take into consideration the firms' current market power – i.e., it should be 'lower' than current market license rate. Finally, in *Rambus*, the EU Commission introduced a maximum royalty cap, thus directly determining the maximum compensation that the parties could receive to grant access to the facility. However, *Rambus* seems to be a rather exceptional case: the EU Commission has rarely directly set the license rate in its antitrust and merger Decisions.

4.3.c. 'Reasonable' license rate in B2B data sharing

Most of the methods discussed in Section 4.3.a. regarding how a 'reasonable' royalty rate can be estimated in order rely on the role played by the standard so as to determine the SEP license rate. This is the case for the *ex-ante* incremental value approach as well as for the top-down approach. In the context of B2B data sharing, industry standardization implies the definition of common APIs to ensure the portability of data and the compatibility of different datasets. In other words, industry standardization does not have an impact on the value of the dataset. By contrast, the logic of the benchmarking approach could be applied, *mutatis mutandis,* in the context of B2B data sharing. The data holder may be required to apply the same rate when it grants access to a specific dataset to different parties. As discussed in the previous section, the benchmarking approach would be applicable only if the licensed dataset is the same and if the contractual conditions of the different data sharing agreements include similar conditions. Finally, the customers' surveys that form the basis of the 'present value-added' and 'hedonic pricing' methods might be applied, *mutatis mutandis,* to determine a 'reasonable' rate for B2B data sharing: such a survey would measure the customers' willingness to pay to gain access to a specific dataset. Surveys among potential data recipients might be useful to determine the perceived value of gaining access to the datasets in different industries. As discussed in Section 2, the value of the dataset is not just measured by the amount, variety and quality of the data included in it, but, rather, by the way in which the recipient can use the data to improve the quality of its products and to cut its production costs. In other words, the value of the dataset is rather individual, and it is different for each data recipient. Since firms operating in different industries would value the same dataset in a different way, a market survey would be a useful tool whereby to determine the rate that is considered 'reasonable' for firms operating in different industries.

The access remedies imposed by the EU Commission under Art. 102 TFEU and merger control, allow us to draw some useful lessons as to how to determine a 'reasonable' compensation rate in B2B data sharing. Firstly, considering *Microsoft* Decision, a 'reasonable' rate should not include the 'strategic value' that is derived from the data holder's market power. In other words, in a case in which the data holder has substantial market power, a 'reasonable' compensation rate should be 'lower' than the license rate that is otherwise requested by the data holder from third parties. Secondly, considering *Siemens/Drägerwerk* and *Newscorp/Telepiù* Decisions, the 'reasonable' remuneration rate might be estimated by looking at the costs faced by the data holder. While the marginal costs faced by the data holder, to grant access to the dataset by an additional recipient would be minor (i.e., probably close to zero), the compensation could include the costs faced by the data holder in maintaining and updating the dataset - i.e., long running incremental costs. Thirdly, looking at the recent *Insurance Ireland* decision, a 'reasonable' compensation should be estimated looking at the effective data access exercised by the third party. In addition, as mentioned in the *Insurance Ireland* decision, a 'reasonable' fee might include a "one-time on-boarding fee" to compensate the data

(Case No COMP/M. 2876 *Newscorp / Telepiù*).

361 *Ibid,* Annex on commitments, para. 11.6.

holder for the costs faced in setting up the dataset.

The access costs approach is also endorsed by proposed Data Act, which has the main method of determining a 'reasonable' royalty rate when the recipient is an SME.[362] In such a case, the data holder can only ask for compensation for the "direct cost of making the data available" to the SME.[363] According to the Data Act's preamble, the direct costs include "the costs necessary for data reproduction, dissemination via electronic means and storage, but not of data collection or production."[364] Therefore, the Data Act proposal differentiates the assessment of the 'reasonable' compensation on the basis of the data recipient: while SMEs should only be asked to pay the marginal cost of access the dataset, other recipients might be required to pay a 'higher', but still 'reasonable', compensation. For example, the latter compensation might include the costs faced by the data holder to update and maintain the dataset. In addition, the benchmarking approach and market surveys might also provide an indication of a 'reasonable' rate.

Unlike the Data Act proposal, the DMA and the sector-specific regulations on mandated B2B data sharing do not provide any indication of the methods that should be relied on to estimate a 'reasonable' royalty rate. The Motor Vehicle Regulation, for instance, mentions that the car manufacturer should calculate the fee to provide access to the vehicle diagnostic data to independent repairs either on the time of access (i.e., hourly, daily, monthly or annual basis) or on the basis of the number of access times.[365] On the other hand, the Regulation does not provide any concrete indication of the possible methods that a car manufacturer could follow to define a reasonable access rate. The benchmarking, customers surveys and estimation of access and maintenance costs could be useful methods to this regard.

Finally, it is worth to bear in mind that the methods followed in the context of SEP licensing and competition law remedies to define a 'reasonable' license rate should take in consideration the peculiarities of B2B data sharing. Firstly, firms often grant access to their dataset either in exchange of specific services from the data recipient (e.g., data analytics) or in exchange of other data; cross-licensing of data in rather common in B2B data sharing. In addition, intermediaries play an important role in B2B data sharing: data platforms and technical enablers act as intermediaries between different business actors that would like to exchange data. Intermediaries often ask the recipient to pay a standard subscription fee, rather than asking for the payment of an ad-hoc fee, based on the amount of data accessed by the recipient. While cross-licensing is also a common practice in SEP licensing and it could thus be taken in consideration to assess a 'reasonable' data sharing rate, the presence of intermediaries is a key-difference between SEP licensing/competition law remedies and B2B data sharing and it would make more complicate the assessment of a 'reasonable' rate.

To sum up, some of the methods elaborated in the context of SEP licensing and competition law remedies may provide some guidelines on how to estimate a 'reasonable' license rate in the context of B2B data sharing. By comparing the fee previously charged by the data holder to other recipients (i.e., benchmarking), conducting surveys among potential data recipients operating in different industries, and estimating the access and maintenance costs faced by the data holders, are examples of possible methods that can be used to estimate a 'reasonable' rate in the context of B2B data sharing. While the proposed Data Act endorses the marginal access cost approach when the recipient is an SME, the DMA, and the other sector-regulation mandating B2B data sharing does not provide any clarification on how to calculate a 'reasonable' access rate. As Justice Birss argues in *Unwired Planet,* no single method can provide the 'right' rate; cross-checking the 'reasonable' rate using different methods is considered to be a better approach.[366] Finally, it is worth bearing in mind that the peculiarities of B2B data sharing should also be borne in mind: cross-data licensing and the presence of a market intermediary would make more complex the application of the methods

362 *Supra,* Art. 9(2) Data Act proposal.
363 *Supra,* para. 42 preamble Data Act proposal.
364 *Supra,* para. 44 preamble Data Act proposal.
365 *Supra,* Art. 63(2) Regulation 2018/858.
366 *Supra,* [2017] EWHC 711.

mentioned above.

4.4. 'Non-discriminatory' license conditions

4.4.a. 'Non-discrimination' in SEPs licensing

In the context of debate on the meaning of FRAND in the context of SEPs licensing, economists have discussed the meaning of the 'ND prong', debating around which circumstances might the SEP holder discriminate against its licensees. Three interpretations of the non-discrimination obligation have been put forward in the literature. The first considers the non-discrimination obligation to be an 'absolute' obligation for the SEP holder: after having accepted the FRAND commitment, the patent holder should license the essential patent to every licensee at the same royalty rate and under the same licensing conditions.[367] According to this interpretation, the non-discrimination principle is *de facto* equivalent to a Most Favorite Nation (MFN) obligation:[368] when the SEP holder concludes a license agreement, it will have to grant the same conditions to other licensees in any further agreement, independently of the specific circumstances of each case. The MFN approach will create a level-playing field among all licensees; on the other hand, it would be a rather inefficient approach.[369] Firstly, aware of the MFN obligation, the SEP holder would initially ask for a 'high' royalty rate; 'higher' than the average rate that the patent holder would be likely to demand if they were able to discriminate amongst its licensees. Secondly, the royalty rate would remain 'fixed', independently by the long-term success/failure of the retail products that were implementing the patented technology. After some time, the patented technology would inevitably be outdated by new technological developments. However, due to the MFN obligation, the SEP holder would be forced to keep the same royalty rate, though no implementer would be interested in licensing the patent any longer. The MFN approach is thus inefficient since it does not incentivize the diffusion of the patented technology and does not adapt to market and technological developments. In addition, the MFN approach is also 'unfair':[370] an implementer, manufacturing products where the essential patent has only a marginal importance, will have to pay the same royalty rate as another implementer, which manufactures products that mostly rely on the essential patent. In view of its inefficiency and its unfairness, it is not surprising that the MFN interpretation of the ND prong has not been supported by any of the authors in the literature.

A second interpretation of the non-discrimination obligation has been put forward by Mariniello.[371] Mariniello suggests that "the FRAND commitment waives the patent holder's right to refuse to license its IP rights to anybody seeking such a license".[372] On the other hand, the patent holder could vary the royalty rate on the basis of the specific circumstances of each licensee.[373] As Justice Birss recognized in *Unwired Planet,* this interpretation "… is very weak. Since the FRAND undertaking already obliges licensors to offer licenses to everyone, it does not add anything."[374] In view of these considerations, it is not surprising that no other author has supported the view expressed by Mariniello.

367 Gregory Sidak (2017), "Fair and Unfair Discrimination in Royalties for Standard-Essential Patents Encumbered by a FRAND or RAND Commitment" 2 *The Criterion Journal on Innovation: pp.*301-370. P. 316.

368 The expression 'Most Favourite Nation (MFN) obligation' derives from international trade law. In particular, in the context of the WTO/GATT rules: when State A concludes a trade agreement with State B that lowers the bilateral custom duties and/or limits an important quote, State A is required to extend the same condition to any other WTO Member State.

369 *Supra*, [2017] EWHC 711, para. 497.

370 Richard Gilbert (2011), 'Deal or No Deal – Licensing Negotiations in Standard-Setting Organizations' 77(3) *Antitrust Law Journal:* 855-888. At 875.

371 Mario Mariniello (2011), 'Fair, Reasonable and Non-Discriminatory (FRAND) Terms: A Challenge for Competition Authorities' 7(3) *Journal of Competition Law and Economics:* 524-541.

372 *Ibid,* p. 525.

373 *Ibid,* p. 532.

374 *Supra,* [2017] EWHC 711m para. 498.

According to the third interpretation of the ND prong, the non-discrimination obligation is applicable only if the licensees are 'similarly situated'. Such an interpretation was first proposed by Gilbert in 2011;[375] Gilbert, however, did not define when licensees are 'similarly situated'. Other authors have built upon the concept introduced by Gilbert. According to Carlton and Shampine, "… competing firms are similarly situated if, *ex ante,* they expect to obtain the same incremental value from the patented technology compared with the best alternative available to be incorporated into the standard."[376] The expectation should be formed *ex-ante* – i.e., before the standard is defined within the SDO. The test elaborated by Carlton and Shampine would be quite difficult to apply in practice. As discussed in the previous sub-section, industry standards are usually developed quite far ahead of the release of those retail products that implement them. It would therefore be quite difficult for the implementers to determine, *ex ante,* the value of the patented technology and thus to assess whether two potential licensees are indeed 'similarly situated'. Other authors have argued in favor of a 'narrow' interpretation a 'similarly situated' standard. In this regard, Sidak recognizes that licensees are similarly situated only if they implement the relevant standard in products in the same market (i.e., competing products).[377] Secondly, different implementers are 'similarly situated' only if the license agreements concern the same patents portfolio.[378] Thirdly, licensees would be 'similarly situated' only if the cost of licensing that is faced by the SEP holder were to be comparable in both transactions (e.g., the same negotiation time for different license agreements).[379]

A number of British and German courts have discussed the scope of application of the ND prong in SEP disputes. Most of the tribunals have pointed out that the principle of non-discrimination is applicable only to 'comparable situations', thus endorsing the 'similarly situated' licensee standard.[380] However, national courts have generally failed to discuss the circumstances under which two licensees are 'similarly situated' – i.e., they have not clarified whether they opt for a 'narrow' or 'broad' interpretation of the similarly situated standard.

German courts, however, have introduced a far-reaching interpretation concerning the applicable burden of proving discriminatory behavior by the SEP holder. In *Sisvel v. Haier,* the *Düsseldorf Oberlandesgericht* (OLG, Düsseldorf Higher Regional Court) pointed out that the burden of proof lies with the party putting forward the allegation of discriminatory behavior by the SEP holder (i.e., the potential licensee).[381] Nevertheless, the Court also recognized that the licensee does not have any regular knowledge of the license practice of the SEP holder, since negotiations are usually conducted at a bilateral level.[382] Consequently, when the potential licensee puts forward an allegation of discriminatory behavior, the SEP holder has the duty to provide evidence about the terms previously agreed upon with other licensees.[383] German courts have thus recognized a *de facto* 'disclosure' obligation by the SEP holder concerning the royalty rates that have been previously agreed with other licensees in relation to a specific patents portfolio. The LG Dusseldorf has further emphasized that the disclosure should be 'full' – i.e., providing detailed information about the license conditions, as well as the names of the parties with whom the SEP holder has previously concluded a license agreement.[384] In the case that the disclosed documents have provided *prima facie* evidence of discrimination, it would be up to the SEP holder to justify the different treatment by explaining that the potential licensee was not 'similarly situated' to the previous licensees.[385] The disclosure obligation by the SEP holder might affect trade secrets. In view of this consideration, OLG Karlsruhe has also

375 *Supra,* Gilbert, p. 875.
376 Dennis Carlton, Alan Shampine (2013), 'An Economic Interpretation of FRAND.' 9(3) *Journal of Competition Law and Economics*: 531. At p. 546.
377 *Supra,* Sidak (2017), p. 359.
378 *Supra,* Sidak (2017), p. 361.
379 *Ibid,* p. 363.
380 See, for instance:
- LG Dusseldorf, case n. 4c O 81/17, ruled on 11.07.2018. para. 271.
- LG Dusseldorf, case n. 4a O 15/15, ruled on 9.11.2018. Para. 392.
381 OLG Düsseldorf, case n. I-15 U 66/15, 30.03.2017, para. V.2.d.aaa.
382 *Ibid*.
383 *Ibid.*
384 *Supra,* LG Düsseldorf, 4a O 15/15, para. 393.
385 OLG Düsseldorf, case n. I - 2 W 8/18, ruled on 25.04.2018.

pointed out that the SEP holder is not required to make public the license agreements previously concluded with other licensees but, rather, has to provide detailed information about the different licensing 'offers', in order to compare them in court proceedings and to ensure that they are not discriminatory.[386]

To sum up, most of the economists have endorsed the 'similarly situated' standard to assess cases of discrimination in the context of SEP disputes. However, neither economists nor national courts have ever clarified the circumstances under which two licensees are similarly situated. German courts have introduced a reversed burden of proof in cases of *prima facie* discrimination, to compensate for the information asymmetry between the SEP holder and the potential licensee.

4.4.b. Non-discrimination in EU competition law remedies

As mentioned in Section 4.3.b., Rambus committed to licensing its portfolio of patents that are relevant to the implementation of the DRAM standard, based on the most-favored license basis.[387] *Rambus is,* however, a rather isolated case; it is the only Decision in which the EU Commission has applied the MFN interpretation of the non-discrimination obligation. Rather, in its antitrust and merger Decisions, the EU Commission has opted for the 'similarly situated' standards, as most experts and national courts interpret the meaning of the non-discriminatory commitment in the context of SEP licensing. In its 2004 Decision, for instance, the EU Commission required Microsoft to license its interoperability information only to firms providing "work group server operating system products" – i.e., Microsoft's direct competitors.[388] Similarly, in the recent *Google-Fitbit* decision, the merging parties committed to granting access to core interoperability APIs to competing manufacturers of smart watches and wearable devices, in order to ensure Android system compatibility for devices that are produced by Fitbit competitors.[389]

Except for *Rambus,* the EU Commission Decisions seem to interpret the 'similarly situated' standard as referring to the direct competitors of the parties who are subject to the remedies. The EU Commission has thus opted for a rather 'narrow interpretation' of the 'similarly situated' standard, compatible with the view expressed by Sidak on how to interpret the non-discrimination prong of FRAND in the context of SEP licensing.[390] Finally, it is worth mentioning that the EU Commission has never introduced a reversed burden of proof on discrimination that is comparable to the approach followed by the German courts, as discussed in the previous pages.

4.4.c. Non-discrimination in B2B data sharing

As discussed in Section 2, B2B data sharing may take place between firms active in the same industry, where the data recipient provides complementary services to the data holder, but also between among operating across different sectors. Data re-use by firms operating in different industries could stimulate innovation by allowing the data recipient to launch new services into the market. The scope of the non-discrimination obligation across different industries is thus a key question in this regard.

Both in competition law and in SEP licensing, the SEP/assets' holder is required not to discriminate against third parties if the latter are 'similarly situated'. The prevailing view, both in competition law and in the context of SEP licensing, is that parties are similarly situated only if they are direct competitors. If we apply this logic to B2B data sharing, the data holder could charge different rates to data recipients operating across different industries, since they are not direct competitors. This interpretation is endorsed by the wording of the proposed Data Act. According to Art. 8(3) of the proposed Data Act, in fact, the data holder 'shall not discriminate between comparable categories of data recipients.' The preamble of the proposed Data Act does not clarify the meaning of "comparable

386 *Ibid,* para. 134.
387 *Supra,* EU Commission Decision in *Rambus,* Annex on commitments, para. 49(e).
388 *Supra,* EU Commission Decision in *Microsoft,* para. 1006.
389 Commission Decision of 17.12.2020 declaring a concentration to be compatible with the internal market and the EEA agreement (Case M.9660 – GOOGLE/FITBIT). Annex on commitments, para. 10.
390 *Supra,* Sidak (2017).

categories of data recipients". However, as Habich argues,[391] by looking at the wording of the preamble, we might conclude that data recipients operating in different industries are not similarly situated, and thus they may be subject to different remuneration conditions by the data holder. Besides possible discrimination among the recipients operating in different industries, the wording of the proposed Data Act would also support different treatment for SMEs and for other categories of data recipients. As discussed in the previous pages, the proposed Data Act generally allows 'better' contractual terms in a case in which the data recipient is an SME (e.g., a 'reasonable' rate based on the marginal cost of access to the dataset). The data holder could therefore ask for a lower compensation rate from the SMEs than from other data recipients.

The Digital Markets Act follows a similar approach in relation to the interpretation of the non-discrimination obligation. Art. 6(11) DMA, in fact, requires the gatekeeper to share ranking, query, click and view data, on FRAND terms only, with "undertakings providing online search engines." Similarly to the proposed Data Act, the DMA thus endorses a 'narrow interpretation' of the ND prong in the case of mandated B2B data sharing. The gatekeeper, in other words, is required to apply the same sharing conditions *vis-à-vis* competing search engines, while it could charge different non-FRAND rates to other digital firms. The other EU sector-regulation mandating B2B data sharing refers to the principle of non-discrimination but without clarifying its precise meaning. Taking into consideration the wording of the proposed Data Act and of the DMA, as well as the prevailing interpretation of the ND prong in SEP licensing and competition law remedies, we might conclude that the non-discriminatory obligation within sector-regulation would only be applicable to data recipients competing within the same relevant market.

The procedural tools elaborated by German courts to reverse the burden of proof between the parties may have a useful application in the context of B2B data sharing. The data holder could be required, either by a national court or by the FRAND disputes settlement body which is provided for in the proposed Data Act, to disclose the terms and conditions of previous data sharing agreements. The data holder would not be required to disclose trade secrets and confidential information but, rather, to provide a summary of the conditions previously agreed with third parties. In cases where the conditions diverged, both in terms of tariffs and other contractual terms, it would be up to the data holder to explain why the potential data recipient is not similarly situated to those other parties with whom it had previously concluded a sharing agreement.

The reversed burden of proof of non-discrimination has been introduced in the proposed Data Act: in the case of *prima facie* discrimination, in fact, it is up to the data holder to show that the diverging contractual conditions are justified for "objective reasons".[392] The proposed Data Act does not explain what valid justifications can be put forward by the data holder. However, in view of the points discussed above, the data holder could probably justify a case of *prima facie* discrimination that benefits SMEs, if compared to other data recipients. Similarly, the data holder could justify the diverging access rates requested by recipients operating in different industries, since the latter are not 'similarly situated' and thus can be discriminated against by the data holder.

The reversed burden of proof is not mentioned in any other EU legislation on mandated B2B data sharing. However, this procedural tool could be applied, *mutatis mutandis,* by those courts and arbitration tribunals that, in the future, will have to interpret the meaning of the NG prong in FRAND disputes in the context of B2B data sharing.

391 *Supra,* Habic (2022), at 1353.
392 *Supra,* preamble proposed Data Act, para. 41.

5. Conclusions

As mentioned at the beginning of the paper, data is the oil of the 21st economy: in the context of the digital economy, in fact, firms are competitive only if they have access to a large amount of high-quality data. Similarly, public institutions can provide more personalized services to citizens if they can access a large dataset. However, small firms and public institutions can often not collect a sufficiently large amount of data on their own; via data sharing, small firms and public institutions can have access to larger and more diversified sets of data, thus boosting their efficiency. Data access/re-use not only increases the efficiency of the data recipient; it is a win-win strategy for the data holder too. The latter, in fact, could gain remuneration for the shared data. In the case of data re-use, the dataset would represent a sort of 'waste product' for the data holder, since the latter would not further rely on such a dataset. By contrast, the recipient could 'recycle' the dataset to develop new and innovative services. As discussed throughout the paper, the compensation received by the data holder would not be limited to monetary compensation: the recipient could also exchange its data with the data holder. Alternatively, the recipient could provide data analytics services to the data holder in exchange for the shared data. In a nutshell, data 'access' and 're-use', which are jointly defined in this paper as 'data sharing', are efficient practices both for the data holder and the data recipient. This is the case in business2business (B2B) scenarios, as well as in government2business(G2B) and business2government typologies of data sharing.

It is also worth pointing out that an increased degree of data sharing between public and private actors would not harm the privacy of individuals. The strict GDPR requirement on the collection and processing of personal data would continue to apply. In particular, the sharing of personal data may take place either if the data subject has provided his/her consent, or if the data has been anonymized, and has thus moved outside of the scope of data protection rules.

Despite its great benefits, the degree of data sharing is still limited. In spite of its growth during recent years, there are several firms/institutions that do not share their data with third parties. Data sharing is rather common among high tech firms, utilities and the providers of financial services, while public agencies, pharmaceutical companies and health care providers rarely grant access to their datasets to third parties. Several reasons explain the 'data sharing paradox': interoperability and data portability obstacles, security and privacy concerns, uncertainty about the applicable legal framework, as well as a few market failures that are obstacles to the data sharing process. Due to the lack of well-functioning data markets, firms/public institutions cannot assess the value of their datasets. They often prefer to 'seal' their data, therefore, rather than sharing with third parties.

In recent years, the European Union has developed a new legal framework to boost B2B, as well as G2B and B2G data sharing. The new legal framework includes 2 layers: on the one hand, the progressive establishment of Common European Data Spaces aims to introduce common standards in strategic sectors to foster interoperability and to solve security and privacy concerns via *ad hoc* industry solutions. On the other hand, a common cross-sectoral legal framework increases legal certainty and removes the market failures that hamper the sharing process. Within this new legal framework, while the Data Governance Act (DGA) and the Open Data Directive (ODD) aim to stimulate G2B data sharing, the recently proposed Data Act aims to foster B2B and B2G data sharing. Similarly, the right of data portability, under Art. 20 GDPR, also strengthens the B2B data sharing of personal data, and it thus complements the right of portability of non-personal data under Art. 5 of the proposed Data Act. Finally, the EU has adopted an increasing number of pieces of legislation mandating B2B data sharing in specific sectors. The Digital Market Act, for instance, includes a number of specific data sharing obligations, mandating digital gatekeepers to share their data with competitors under certain circumstances. The DMA complements sector-specific rules, which mandate data sharing in specific industries, such as in the chemical, banking, automotive, electricity, telecoms, and postal sectors.

The present paper has analysed the emerging EU *acquis* on data sharing, comparing the provisions on terms and compensation that are included in the legislation mentioned above. The EU legal framework refers to 3 main typologies of compensation: 'free access'; fee based on marginal cost of data sharing; Fair, Reasonable and Non-Discriminatory (FRAND) compensation. A fourth typology, which is defined in this paper as 'quasi-FRAND', refers to situations in which the EU legislation demands a non-discriminatory and proportional compensation for the data holder; however, the FRAND formula is not fully and properly mentioned in such legislation.

This paper has highlighted a few inconsistencies in the way data sharing compensation is formulated in the different pieces of legislation. In the context of G2B data sharing, for example, while the ODD points out that data sharing should take place 'free of charge', the DGA opts for an access costs compensation mechanism. Secondly, in the context of data portability in B2B data sharing, the GDPR and the proposed Data Act diverge in relation to the applicable rules on compensation: on the one hand, the controller should transfer the personal data to any third party 'free of charge'. On the other hand, under the proposed Data Act, the compensation paid by the recipient to the data holder should be FRAND-based. As argued throughout the paper, since the FRAND formula safeguards both the interests of the recipient (to allow them access to the dataset), as well as rewarding the data holder for their efforts in collecting and establishing the datasets, 'free of charge' compensation could hardly be considered compatible with the FRAND formula. Art. 20 GDPR and Art. 5 of the proposed Data Act clearly diverge in terms of compensation. Due to the increasing 'blurring' of the distinction between personal and non-personal data, the difference between the two pieces of legislation may create, in the future, some degree of legal uncertainty in relation to the appropriate data sharing compensation. A third example of inconsistency concerns the compensation formula provided by the different EU legislation concerning mandated B2B data sharing: while the DMA, REACH, Motor Vehicles Regulation and the EECC clearly refer to the FRAND formula, the PSD2, the Electricity and the Postal Services Directives refer to the basic logic of FRAND, without mentioning the proper wording of this 'magical' formula (i.e., the 'quasi-FRAND' formula). Due to the increasing overlap between different sector legislations, the co-existence of the FRAND and quasi-FRAND formulae may generate legal uncertainty, and thus harm B2B data sharing.

Section 4 of the paper has analysed the meaning of the FRAND principle in the context of B2B data sharing. The proposed Data Act, the DMA, and the EU sector legislation mandating B2B data sharing, do not fully clarify the meaning of this 'magical' formula. Since FRAND often appears in different EU legislations, it may be considered a general principle of EU law. Its meaning in B2B data sharing can therefore be interpreted by looking at the lessons drawn in the application of the FRAND principle in other policy areas. In the present paper, we have analysed the meaning of FRAND in the context of the licensing of Standard Essential Patents (SEPs) and in competition access remedies, to understand how FRAND might be interpreted in the context of B2B data sharing.

The paper has argued that, except for the first two steps, the *Huawei v. ZTE* negotiation framework could be applicable, *mutatis mutandis,* to the case of B2B data sharing. The framework, as further interpreted by the case law from a number of German courts, provides useful indications with which to assess whether the data holder and the recipient have behaved 'fairly' during the negotiations.

Secondly, the paper has argued that some of the methods elaborated in the context of SEP licensing and in competition access remedies to define a 'reasonable' license rate, could be applicable in the context of B2B data sharing. Comparing the fee previously charged by the data holder to different recipients (i.e., benchmarking), conducting surveys among potential data recipients operating in different industries, and estimating the access and maintenance costs faced by the data holders, are examples of possible methods that might be used to estimate a 'reasonable' access rate in the context of B2B data sharing.

Finally, the paper has noticed that, both in SEP licensing and in competition access remedies, the non-discrimination prong of the FRAND principle is applied only to third parties that are 'similarly situated'. Only competitors within the same relevant market may be 'similarly situated'. This approach could be applied also in the context of B2B data sharing: as already provided for in the proposed Data Act, the data holder could charge a lower fee to SMEs in comparison to that charged to a non-SME data recipient. Similarly, firms operating in different industries would not be 'similarly situated', and thus the data holder could apply different terms and conditions. Last, but not least, the reversed burden of proof developed by a number of German courts in relation to the application of the non-discrimination principle in FRAND, could also be applied, *mutatis mutandis,* in the context of B2B data sharing. In the case of *prima facie* discrimination, the data holder should disclose the terms and conditions of previous data sharing agreements and justify them based on the fact that the recipients were not 'similarly situated'.

As argued in previous pages, B2B data sharing shares common features with SEP licensing and antitrust access remedies, but also demonstrates several differences. Monetary compensation is not always the standard rule in B2B data sharing; the recipient often compensates the data holder by providing data analytics services. The non-monetary nature of compensation in B2B data sharing should also be taken into consideration in assessing a 'reasonable' compensation rate. In addition, unlike SEP licensing and antitrust access remedies, B2B data sharing is often characterized by the presence of an intermediary between the data holder and the recipient. The similarities and differences among B2B data sharing, SEP licensing and antitrust access remedies will have to be taken into consideration in the future by those bodies that will be called to adjudicate on disputes involving the application of the FRAND principle in B2B data sharing. In this regard, it is worth noting that Art. 10 of the proposed Data Act establishes specialized disputes settlement bodies to be put in charge of solving FRAND-based disputes in B2B data sharing transactions. The latter bodies will certainly have to look at the case law and experience gained in the context of SEP licensing and antitrust access remedies to clarify the meaning of this 'magical' formula, which is better known as FRAND.

Authors

Marco Botta

European University Institute

marco.botta@eui.eu