The European Data Act

Tombal, Thomas; Graef, Inge

Published in:
From regulating human behaviour to regulating data

Publication date:
2025

From Regulating **Human Behaviour** to Regulating **Data**

Editors
B. van der Sloot, G. Monti & F. Bostoen

OPEN PRESS TiU

CHAPTER

VIII

The European Data Act: A Horizontal Building Block for the Data Economy?

Thomas Tombal &

Inge Graef[1]

https://doi.org/10.26116/w7xa-8288

1 At the time of drafting, Thomas Tombal was a postdoctoral researcher at the Tilburg Institute for Law, Technology and Society (TILT) and the Tilburg Law and Economics Center (TILEC) of Tilburg University, and lecturer at the Université de Namur. At the time of publication, Thomas Tombal works as a Case Handler at the European Commission – DG Competition. The views and opinions expressed herein are personal and do not necessarily reflect those of the European Commission or other EU institutions. Inge Graef is Associate Professor Tilburg Institute of Law, Technology, and the Society (TILT), Tilburg Law School (TLS), Tilburg University.

1. Introduction

The research project underlying this book seeks to study the shift from human-centric regulation to data-centric regulation. The adoption of the Data Governance Act[2] and the Data Act[3] are the most prominent illustrations of how this shift has accelerated in the European context. The Data Act is of particular relevance considering its broad and ambitious scope. Indicative, in this regard, is that the Data Act was heralded as the 'last horizontal building block of the Commission's data strategy'.[4] At the same time, it is a piece of legislation that adds up to an array of existing legislations that aim to regulate

2 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), *OJ L 152/1*, 3 June 2022.

3 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), *OJ L 1/71*, 22 December 2023. For detailed comments of the Data Act, see Kerber, W. (2023). Governance of IoT data: why the EU Data Act will not fulfill its objectives. *GRUR International*, *72*(2), 120-135; Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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). <https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html>; Picht, P. G. (2023). Caught in the acts: framing mandatory data access transactions under the data act, further EU digital regulation acts, and competition law. *Journal of European Competition Law & Practice*, *14*(2), 67-82, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842>, p. 19-42; Colangelo, G. (2022). European Proposal for a Data Act–A First Assessment. *CERRE Evaluation Paper*, available at <https://cerre.eu/wp-content/uploads/2022/07/200722_CERRE_Assessment-Paper_DataAct.pdf>; Habich, E. (2022). FRAND Access to Data: Perspectives from the FRAND Licensing of Standard-Essential Patents for the Data Act Proposal and the Digital Markets Act. *IIC-International Review of Intellectual Property and Competition Law*, *53*(9), 1343-1373; Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *Study for the Ludwig-Fröhler-Institut für Handwerkswissenschaften*, 2022, <https://ssrn.com/abstract=4256882>; Metzger, A., & Schweitzer, H. (2022). Shaping markets: A critical evaluation of the draft data act. <https://ssrn.com/abstract=4222376>; Martens, B. (2023). Pro- and anti-competitive provisions in the proposed European Union Data Act, *Bruegel Working Paper 01/2023*, <https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf>.

4 European Commission, 'Data Act: Commission proposes measures for a fair and innovative data economy' (press release), available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113>. See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, '*A European strategy for data*', 19 February 2020, COM(2020) 66.

the European data economy, whether more horizontal,[5] sectoral[6] or targeted at specific digital actors.[7] Against this background, the chapter critically reflects on the Data Act and its ability to regulate the European data economy effectively. While our analysis goes into the details of the different provisions, our purpose is to show whether the design of key aspects of the Data Act allow it to reach its overall objective of making more data available for use in the EU. As such, this chapter builds up to a wider reflection on the effectiveness of the Data Act for stimulating the European data economy.

We argue that, although the Data Act clarifies important conditions applicable to data sharing more generally and can thereby stimulate the European data economy through the additional clarity provided, its scope is more limited than it may appear at first. The Data Act also leaves certain key issues regarding enforcement and its interaction with other laws unaddressed. On the one hand, this may be a choice of the legislator to channel ambitions considering that the Data Act is a first attempt at a horizontal and legally-binding legislative instrument to regulate the sharing of personal as well as non-personal data. On the other hand, this may be due to the fluid nature of data, the

5 See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), *OJ L 119*, 4 May 2016; 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 November 2018; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information, *OJ L 172/56*, 26 June 2019; Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), *OJ L 152/1*, 3 June 2022.

6 See, for instance, 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, *OJ L 337/35*, 23 December 2015; 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 June 2018; 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 June 2019.

7 See Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019; Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *OJ L 186/57*, 11 July 2019; 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 (Digital Markets Act), *OJ L 265/1*, 14 September 2022; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), *OJ L 277/1*, 19 October 2022.

characteristics and requirements of which change according to the context. In addition, due to its fluid nature, the interactions of data with laws in other areas cannot be fully predicted and clarified upfront beyond a case-by-case setting. As such, the Data Act shows both the potential of regulating a subject matter like data in a horizontal manner as well as its limits, in particular in the form of the remaining need to interpret open questions and to act on a sector-specific basis in parallel. While the Commission may portray the Data Act as 'the last horizontal building block', we believe that its adoption will only just be the end of the beginning of the European data economy's regulation.

According to the Commission, the aim of the Data Act is to address issues that slow down the development of the European data economy, such as the insufficient availability of data for reuse, by aiming to create a legal instrument that would enable wider data use across the economy.[8] This would:

> ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible for all [and would] lead to new, innovative services and more competitive prices for aftermarket services and repairs of connected objects.[9]

In order to achieve these objectives, the Data Act combines two approaches. On the one hand, the Data Act imposes specific new data access obligations on businesses, including in the context of Internet of Things (IoT) devices,[10] regulates the sharing of data to public sector bodies in cases of exceptional need[11] and facilitates the switching of data processing services in the cloud environment.[12] On the other hand, the Data Act creates a baseline horizontal framework for compulsory data sharing. This chapter focuses on the latter.

The baseline horizontal framework for compulsory data sharing is at the heart of section 2 of this chapter in particular. It concerns the basic common rules that will need to be applied in any situation where a legislation adopted or revised after the Data Act makes it compulsory for a data holder to make data available to a data recipient.[13] Accord-

8 Commission Staff Working Document, 'Impact assessment report accompanying the document 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)', Brussels, 23 February 2022, SWD(2022) 34 final, available at <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=SWD%3A2022%3A34%3AFIN&qid=1645811711252>, p. 1 and 7.

9 European Commission, 'Data Act: Commission proposes measures for a fair and innovative data economy', *op. cit.*

10 Articles 4 and 5 of the Data Act.

11 Articles 14 to 22 of the Data Act.

12 Articles 23 to 31 of the Data Act.

13 Article 12.1 of the Data Act. See also Articles 8 to 13. "Data recipient' means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, includ-

ing to its Explanatory Memorandum, the key objective underlying the Data Act's baseline horizontal framework is to contribute to:

> the creation of a cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors.[14]

As this idea of having common horizontal ground rules is a truly novel approach compared to the previous disparate and mostly sector-specific data sharing approaches, we will analyse how the EU legislator has chosen to build this framework, how it aligns with other existing legislation and whether there are still potential gaps.

Section 3 focuses on enforcement, which is relevant for the Data Act's horizontal framework for compulsory data sharing and for the specific new data access obligations it imposes on businesses. The issue of enforcement is only briefly addressed in the Data Act.[15] However, we believe that many uncertainties result from the text, which could hamper the Data Act's objective of fostering more data sharing in the EU. The provisions could lead to scattered options in terms of the designation of authorities to enforce the Data Act.[16] This could complicate alignment and cooperation between Member State authorities and between authorities within the same Member States, as more than one authority can be designated to enforce this Act.[17] Since the Member State of the entity's main establishment is responsible for monitoring compliance with the Data Act in cross-border cases,[18] strategic behaviour may occur that in the worst case could lead to a similar enforcement bottleneck as in the GDPR.[19]

Section 4 concludes by summarising our main findings pertaining to the two key aspects of the Data Act. It critically reflects on whether its provisions are suitable to achieve the overall objectives it pursues. In this regard, we also provide an outlook to the future of regulating data sharing in the EU.

ing a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law' (Article 2(14) of the Data Act).

14 Data Act Proposal, Explanatory Memorandum, p. 1.

15 See Articles 37 to 42 of the Data Act.

16 See Article 37 of the Data Act.

17 See Article 37.1 of the Data Act.

18 Article 37.10 of the Data Act.

19 Communication from the Commission to the European Parliament and the Council, '*Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation*', 24 June 2020, COM(2020) 264 final, p. 6; Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *International & Comparative Law Quarterly*, *71*(4), 799-830.

2. The Data Act's Baseline Horizontal Framework for Compulsory Data Sharing

The key objective of the Data Act – to create a cross-sectoral (horizontal) framework for compulsory data sharing – might seem quite broad at first. The Data Act can potentially be understood as applying to any type of compulsory data sharing between businesses and their users (B2U data sharing), between businesses (B2B data sharing), between businesses and public sector bodies (Business-to-Government (B2G) and Government-to-Business (G2B) data sharing), and between public bodies (Government-to-Government (G2G) data sharing). However, the scope of this horizontal framework is much more limited, as we outline below. Beyond this, it is clear that legislation that organises voluntary data sharing, such as the Data Governance Act,[20] will remain unaffected by the Data Act's horizontal framework.[21]

2.1 Scope of the Framework

The Data Act's horizontal framework only applies where a data holder is obliged to make data available to a data recipient.[22] Data holders are the actors who have de facto or de jure control over data generated by products or services, and who have the obligation under EU law to make available certain data.[23] This suggests that only businesses that collect data through their control on products or services fall within the scope of this horizontal framework. Accordingly, this would exclude G2B and G2G data sharing from this framework. Here, we can see a clear distinction with the Data Governance Act, which contains a broader definition of 'data holders' as public sector bodies are also covered.[24]

---

20 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), *OJ L 152/1*, 3 June 2022.

21 Recital 42 of the Data Act.

22 Article 12.1 of the Data Act.

23 Article 2(13) and Recital 5 of the Data Act.

24 See Article 2(8) of the Data Governance Act: "data holder' means a legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data'. According to the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), this discrepancy between the two regulations could create some confusion and legal uncertainty. EDPB-EDPS, *Joint Opinion 2/2022 on the Proposal of the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, 4 May 2022, available at <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en>, p. 11.

Data recipients are defined by the Data Act as 'legal or natural person[s], acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service'.[25] This would thus exclude B2G data sharing (as public sector bodies do not act for purposes related to trade, business, craft or profession) and B2U data sharing (as users are explicitly excluded) from the scope of this horizontal framework. It therefore only applies to compulsory B2B data sharing, which is confirmed by the Commission itself.[26] Note, however, that B2B data sharing can take place at the initiative of the user when invoking a right to move data from one business to another business.

Looking at the three data sharing obligations contained in the Data Act as mentioned in the introduction, this means the horizontal framework only applies to the IoT data access right to the extent that it benefits third parties,[27] but not to the extent that it benefits the users of connected products or related services,[28] as that is a B2U data sharing scenario. Furthermore, it does not apply to data sharing for exceptional need,[29] as this constitutes B2G data sharing. It does not apply to data portability obligations imposed on providers of data processing services either,[30] as the Data Act does not provide for the possibility of direct data sharing between the provider and a third party. Instead, it only provides for data sharing between the provider and its users (B2U data sharing). These cases fall outside of the horizontal framework and thus require targeted rules.

Importantly, the horizontal framework also does not apply to all legislation imposing B2B data sharing. Instead, it only applies to obligations to make data available under EU legislation or national legislation that implements EU law that will enter into force after 11 January 2024.[31] Therefore, this framework will not apply to any pre-existing (sectoral) legislation imposing compulsory B2B data sharing, such as Article 20.2 GDPR.

The Data Act's horizontal framework for compulsory data sharing is thus much narrower than it might appear at first sight. Accordingly, some uncertainty might remain

25 Article 2(14) of the Data Act. According to the EDPB and the EDPS, the Data Act should specify whether data intermediation services, as defined in Art. 2(11) of the Data Governance Act, are covered as recipients, as Recital 35 of the Data Act Proposal seems to suggest (EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, p. 11-12).

26 Commission Staff Working Document, 'Impact assessment report accompanying the Data Act', *op. cit.*, p. 68.

27 Article 5 of the Data Act.

28 Article 4 of the Data Act.

29 See Articles 14 to 22 of the Data Act.

30 See Articles 23 to 31 of the Data Act.

31 Article 12.1 and 44.1 of the Data Act.

in the coming years due to the parallel application of different rules and regimes. This is not tenable in the long term, and some convergence between the Data Act's horizontal framework and other data sharing instruments will have to be achieved in the future.

Finally, it is important to outline that this is a baseline horizontal framework. This implies that the rules it contains lay down the minimum standards applicable to any legislations that fall within its scope. However, it does not prevent the adoption of more specific and far-reaching rules in the context of individual sectors or that of the development of common European data spaces.[32] These more specific rules could, for example, include further-reaching requirements on technical aspects of the data access,[33] on limits to the data holder's right to use certain data provided by users or on other aspects that go beyond data access matters.[34] In this regard, it will be important to find the right balance between accommodating sector-specific needs and maintaining a minimum level of coherence between the different instruments to avoid the creation of a patchwork of data sharing regimes that would be hard to navigate.

2.2 Framework Design

2.2.1 The Central Role of Data Sharing Agreements

The cornerstone of this horizontal framework is that data holders have to share the data with data recipients in a transparent manner and under fair, reasonable and non-discriminatory (FRAND) terms, through the means of a data sharing agreement.[35] Importantly, the Data Act underlines that the principle of contractual freedom must be respected. Accordingly, it will be up to the parties involved to negotiate these terms and to agree on what constitutes FRAND terms in their particular situation.[36] Some argue that this contractual path is questionable as 'it increases transaction costs for data recipients who cannot obtain the data directly via an open interface or in other auto-

32 Article 44.2 and Recital 115 of the Data Act. See, for instance: Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, 3 June 2022, COM(2022) 197 final.

33 Such as 'interfaces for data access, or how data access could be provided, for example directly from the product or via data intermediation services' (Recital 115 of the Data Act).

34 Article 44.2 of the Data Act.

35 Articles 8.1 and 8.2 of the Data Act. According to the EDPB and the EDPS, the fact that the data subject, whose data might be shared, plays no role in the elaboration of such contract 'risks to severely compromise the effectiveness of data protection rights' (EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, p. 17). For some, this unilateral formulation against the data holder is problematic and the data recipients should also be under the obligation to negotiate FRAND terms in good faith (see Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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) *op. cit.*, p. 39).

36 Recital 43 of the Data Act.

mated ways'.[37] This is because, while 'negotiations may lead to efficient results in the B2B area if the companies are on the same level and there are no power asymmetries', requiring a contractual agreement creates 'considerable potential for disrupting free access to data, since remuneration and conditions are to be negotiated by parties with very different bargaining positions'.[38]

Despite this, the parties' contractual freedom is limited to the extent that the data sharing agreement terms may not exclude the application of this horizontal regime, derogate from it or vary its effect.[39] These rules are imperative, and any contractual term that does not comply with them shall not be binding on the party to which it is detrimental.[40]

2.2.2 FRAND Requirements

2.2.2.1 *Non-Discriminatory*

In terms of the FRAND requirements, the Data Act provides that the data holder shall not discriminate (i.e. share data at more favourable conditions) between comparable categories of data recipients, including partner and linked enterprises[41] (i.e. engage in

37 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets. *Available at SSRN 4256882*, *op. cit*., p. 27; Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), *op. cit*., p. 29.

38 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets. *Available at SSRN 4256882*, *op. cit*., p. 28. See p. 28-29 for further discussions on this need for a more direct access. See also J. Drexl, C. Banda, B. González Otero, J. Hoffmann, D. Kim, S. Kulhari, V. Moscon, H. Richter and K. Wiedemann, *Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Data Act Proposal*, *op. cit*., p. 28.

39 Article 8.2 of the Data Act.

40 Ibid.

41 "Linked enterprises' are enterprises which have any of the following relationships with each other: (a) an enterprise has a majority of the shareholders' or members' voting rights in another enterprise; (b) an enterprise has the right to appoint or remove a majority of the members of the administrative, management or supervisory body of another enterprise; (c) an enterprise has the right to exercise a dominant influence over another enterprise pursuant to a contract entered into with that enterprise or to a provision in its memorandum or articles of association; (d) an enterprise, which is a shareholder in or member of another enterprise, controls alone, pursuant to an agreement with other shareholders in or members of that enterprise, a majority of shareholders' or members' voting rights in that enterprise' (Article 3.3 of the Annex to the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, *OJ L 124/36*, 20 May 2003); "Partner enterprises' are all enterprises which are not classified as linked enterprises (...) and between which there is the following relationship: an enterprise (upstream enterprise) holds, either solely or jointly with one or more linked enterprises (...) 25 % or more of the capital or voting rights of another enterprise (downstream enterprise)' (Article 3.2 of the Annex to Recommendation 2003/361/EC).

self-preferencing[42]).[43] Importantly, it is up to the data holder to demonstrate that a contractual term is not discriminatory, by proving that a potential difference between two contracts with similar recipients is justified by objective reasons.[44] In this regard, differentiating between recipients from distinct sectors could be justified, as this would 'preserve market-driven incentives to invest in secondary markets with below-average potential of value creation, warranting preferential access conditions for the same input data as other secondary markets'.[45] Some suggest that, in order to verify whether discrimination has occurred, 'it could be required that all previous data access contracts of a company be disclosed to [a specific body]', and that these previous contracts 'could be inspected upon request by arbitration bodies or courts'.[46] Finally, a data holder cannot share data with a data recipient on an exclusive basis unless this has been explicitly requested by a user of the data holder's product or service.[47]

2.2.2.2 *Reasonable*

The Data Act provides that any compensation agreed between the data holder and the data recipient should be reasonable,[48] unless the specific legislation imposing data sharing excludes any compensation at all or provides for a lower one in justified cases.[49] The underlying idea is to incentivise the data holder's 'continued investment

42 On prohibitions of self-preferencing, see also GCEU, *Google Shopping,* 10 November 2021, T-612/17, EU:T:2021:763; Digital Markets Act, *op. cit*., Article 6.5.

43 Article 8.3 of the Data Act.

44 Article 8.3 and Recital 45 of the Data Act.

45 Habich, E. (2022). FRAND Access to Data: Perspectives from the FRAND Licensing of Standard-Essential Patents for the Data Act Proposal and the Digital Markets Act. *IIC-International Review of Intellectual Property and Competition Law*, *53*(9), 1343-1373, p. 1354.

46 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, p. 36.

47 Article 8.4 of the Data Act. As outlined by the EDPB and the EDPS, these non-discrimination and non-exclusivity obligations should however not 'undermine the right of informational self-determination of data subjects according to which they are entitled to discriminate among the recipients of their personal data' (EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal, op. cit*., p. 17).

48 Article 9.1, 9.2 and 9.3 of the Data Act. For a more detailed analysis of what a 'reasonable compensation' could entail, see Monti, G., Tombal, T., & Graef, I. (2022). Study for developing criteria for assessing "reasonable compensation" in the case of statutory data access right: Study for the European Commission Directorate-General Justice and Consumers. <https://data.europa.eu/doi/10.2838/19186>; Habich, E. (2022). FRAND Access to Data: Perspectives from the FRAND Licensing of Standard-Essential Patents for the Data Act Proposal and the Digital Markets Act. *IIC-International Review of Intellectual Property and Competition Law*, *53*(9), 1343-1373, p. 1354-1371. It is also worth noting that the option not to include any compensation for the data holder has been explored but was eventually not retained, due to fears that this would unduly affect the data holders' business interests (Commission Staff Working Document, 'Impact assessment report accompanying the Data Act', *op. cit*., p. 36).

49 Article 9.6 and Recital 50 of the Data Act. Justified cases include 'including the need to safeguard consumer participation and competition or to promote innovation in certain markets' (Recital 50). For instance, the Digital Markets Act provides for a free data portability right (Commission

in generating and making available valuable data, including investments in relevant technical tools'.[50] In fact, the Data Act itself provides for a lower compensation in situations where the data recipient is a micro, small or medium enterprise (SME).[51] The goal is to protect them from excessive economic burdens that would hamper the development of innovative business models.[52] Accordingly, in B2b (the lower case 'b' referring to SMEs) data sharing scenarios, the compensation should not exceed the costs directly related to making the data available[53] and which are attributable to the request.[54] Importantly, this should not be understood as paying for the data itself,[55] but only for the costs incurred for making the data available 'including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage'.[56] The costs may vary depending on the arrangements taken for making the data available:

> Long-term arrangements between data holders and data recipients, for instance via a subscription model or the use of smart contracts, may reduce the costs in regular or repetitive transactions in a business relationship. Costs related to making data available are either specific to a particular request or shared with other requests. In the latter case, a single data recipient should not pay the full costs of making the data available.[57]

The 'reasonable compensation' to be paid by a recipient that is not an SME will necessarily include these direct sharing costs plus a fee covering (at least in part) 'investments in the collection and production of data, where applicable, taking into account whether

Staff Working Document, 'Impact assessment report accompanying the Data Act', *op. cit*., p. 127). Such a distinction can arguably be justified by the fact that the DMA only applies to a limited set of very powerful 'gatekeepers', whose interests should arguably weight less heavily in the balance in light of the market failures they strive on and of the need to foster contestability on those markets.

50 Recital 46 of the Data Act.

51 As defined in Article 2 of the Annex to Recommendation 2003/361/EC.

52 Recital 49 of the Data Act.

53 "Directly related costs are those costs which are attributable to the individual requests, taking into account that the necessary technical interfaces or related software and connectivity will is to be established on a permanent basis by the data holder' (Recital 49 of the Data Act).

54 Article 9.4 and 9.2.a) of the Data Act.

55 Recital 46 of the Data Act. The EDPB and the EDPS have expressed concerns about this reference to 'paying for the data itself', as it would acknowledge the possibility to monetise personal data, while 'data protection is a fundamental right guaranteed by Article 8 of the Charter and personal data cannot be considered as a tradeable commodity' (EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit*., p. 18).

56 Article 9.2.a) of the Data Act.

57 Recital 47 of the Data Act.

other parties contributed to the obtaining, generating or collecting [of] the data in question'.[58] In addition, the compensation 'may also depend on the volume, format and nature of the data'.[59] The reasonable nature of the compensation will thus be a function of the prevailing market conditions and may include a margin, except for SMEs and not-for-profit research organisations.[60] This latter aspect is in line with the Open Data Directive,[61] which further defines a 'reasonable return on investment' as 'a percentage of the overall charge, in addition to that needed to recover the eligible costs, not exceeding 5 percentage points above the fixed interest rate of the [European Central Bank]'.[62] The Data Act is not as specific, which is logical considering the much larger range of situations and types of data it covers in comparison with the Open Data Directive, but it does contain some useful guidance in the recitals. The margin 'may consider the costs for collecting the data'. It may also:

> decrease where the data holder has collected the data for its own business without significant investments or may increase where the investments in the data collection for the purposes of the data holder's business are high. It may be limited or even excluded in situations where the use of the data by the data recipient does not affect the data holder's own activities. The fact that the data is co-generated by a connected product owned, leased or rented by the user could also lower the amount of the compensation in comparison to other situations where the data are generated by the data holder for example during the provision of a related service.[63]

In any case, the data holder will have to provide sufficiently detailed information to the recipient setting out the basis for the calculation of the requested compensation so that the latter can verify that the required compensation complies with the Data Act.[64] This suggests that the initial offer should come from the data holder, allowing the data recipient to make a counter-offer. In this regard, the negotiation framework for the licensing of Standard-Essential-Patents (SEPs) on FRAND terms, as proposed in the Huawei case,[65] could be used as an inspiration to assist the parties in reaching an agree-

58 Article 9.2.b) of the Data Act.
59 Article 9.3 of the Data Act.
60 Recital 47 of the Data Act. See also Commission Staff Working Document, 'Impact assessment report accompanying the Data Act', *op. cit.*, p. 154.
61 Article 6.4 of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information, *OJ L 172/56*, 26 June 2019.
62 Article 2(16) of Directive (EU) 2019/1024.
63 Recital 47 of the Data Act.
64 Article 9.7 and Recital 51 of the Data Act.
65 ECJ, *Huawei*, 16 July 2015, C-170/13, EU:C:2015:477, §§ 60-69.

ment on the remuneration.[66] If no agreement is reached following the counter-offer, the parties should, by common agreement, request that the price be determined by an independent third party (which could be a designated entity [e.g. the Support Centre for Data Sharing[67]]) or a dispute settlement body (e.g. supervising authorities, arbitrators or courts).

An important question underlying this negotiation between the data holder and the recipient is that of the relationship between 'the data holder's right to demand a FRAND compensation for data access [under Art. 8.1] and its access duty to a third party at the request of the user without undue delay [under Art. 5.1]'.[68]

> Allowing the data holder to retain the data until the FRAND dispute is resolved would lead to a violation of the obligation of the data holder vis-à-vis the user and seriously affect the effectiveness of the data access and use right of the latter. Conversely, if one considers the data holder under an obligation to provide access despite its failure to agree on FRAND terms, this would create a so-called 'hold-out' situation, where the third party can simply refuse or evade honest FRAND negotiations, as this will not hinder the provision of the service.[69]

Surprisingly, the Data Act is silent on this tension, even though it is fundamental to ensure that both the holder and the recipient engage in 'diligent and good faith dealing'.[70]

As such, we argue that a balance needs to be found between the interests of data holders and data recipients to ensure effective negotiations. This can be done in different ways. Some have suggested to provide the recipient with immediate access to the

66 Wendehorst, C., & Cohen, N. (2023). ALI/ELI Principles for a Data Economy: Data Transactions and Data Rights. <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf>, p. 177. On this point, see also Drexl, J. (2017). Designing competitive markets for industrial data. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *8*, 257, p. 55; Habich, E. (2022) 'FRAND Access to Data', *op. cit.*, p. 1361-1370; Picht, P. 'Caught in the acts', *op. cit.*, p. 34-36; Tombal, T. (2020). Economic dependence and data access. *IIC-International Review of Intellectual Property and Competition Law*, *51*(1), 70-98, p. 94; Tombal, T. (2022). *Imposing Data Sharing among Private Actors: A Tale of Evolving Balances*, Alphen aan den Rijn, Kluwer Law International (Information Law Series, Vol. 48), p. 298-299.

67 See <https://eudatasharing.eu/>.

68 Habich, E. (2022) 'FRAND Access to Data', *op. cit.*, p. 1358.

69 Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), p. 28.

70 Picht, P. G. (2023). Caught in the acts: framing mandatory data access transactions under the data act, further EU digital regulation acts, and competition law. *Journal of European Competition Law & Practice*, *14*(2), 67-82, *op. cit.*, p. 35.

data in exchange for the deposit of a lump sum.[71] One alternative is to take away the recipient's access to the data if it is found to engage in a manifestly uncooperative behaviour in order to avoid 'hold out' tactics.[72] At the same time, the data holder should not be able to raise a lack of agreement on the 'reasonable compensation' as a way to bypass its duty to share. This would incentivise the data holders to drag their feet and to engage in bad faith negotiations with the recipient by abusing delaying tactics. Even though the Data Act does not specify any such measures, there is still scope to implement the relevant provisions in a way that balances the interests of data holders and data recipients.

In addition, it cannot be excluded that any remuneration charged to data recipients will indirectly affect users as the price paid by third parties to access the data will likely be passed on to them in the cost of the product or service.[73] As this runs counter to the principle according to which data sharing between a holder and a third party should not entail any financial burdens for the user,[74] some argue that the data holder should not be remunerated by third parties either.[75] This would also have the merit to supress the above-mentioned 'negotiation hold-out' issue. The recitals to the Data Act do explicitly leave room for excluding any margin on the part of the data holder (beyond the costs for making the data available under Article 9.2.a) of the Data Act) 'in situations where the use of the data by the data recipient does not affect the own activities of the data holder'.[76] It remains to be seen whether data recipients indeed can convince data holders not to charge any extra margins. This issue is worth monitoring closely, so it is beneficial that the final text of the Data Act requires the Commission to adopt guidelines on the calculation of reasonable compensation in which such issues can be further elaborated.[77]

71 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit.*, p. 36.

72 See Habich, E. (2022). 'FRAND Access to Data', *op. cit.*, p. 1360-1361 and 1368-1370.

73 Martens, B. (2023). Pro-and anti-competitive provisions in the proposed European Union Data Act, *op. cit.*, p. 12.

74 Article 5.1 of the Data Act.

75 J Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), *op. cit.*, p. 38; Martens, B. (2023). Pro-and anti-competitive provisions in the proposed European Union Data Act, *op. cit.*, p. 11; Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit.*, p. 37-38.

76 Recital 47 of the Data Act.

77 Article 9.5 of the Data Act.

2.2.2.3 *Fair*

Moving on to the fair nature of the terms, it must be underlined that 'fairness' is not specifically defined in the Data Act, although an 'unfairness test' has been created for situations where a 'contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations … has been unilaterally imposed by an enterprise on another enterprise'.[78] The Data Act outlines several situations in which contractual terms qualify as unfair or are presumed unfair.[79] Beyond this, it is worth outlining that the Data Act provides that the Commission will develop and recommend non-binding model contractual terms that should assist the parties in drafting balanced data sharing agreements.[80] These model terms, which could take into account specific sectoral conditions and existing practices used in the context of voluntary data sharing mechanisms where necessary,[81] should lead to fairer data sharing contracts.[82]

The horizontal framework also provides rules that ensure that the data sharing obligation does not affect the technical and commercial security of the data holder.[83] First, the Data Act provides information about the articulation with the data holder's trade secrets.[84] This shows that this horizontal framework aims to find a fair balance between the holder's business interests and the benefits that the sharing obligation generates for the recipients. The Data Act provides that an obligation to share data with a data recipient should not oblige the disclosure of trade secrets, unless provided otherwise in the legislation imposing the sharing.[85] It should be outlined here that some believe that 'this

78 Article 13 of the Data Act.

79 Article 13.4 and 5 of the Data Act.

80 Article 41 of the Data Act.

81 See the work of the 'Support Centre for Data Sharing' (https://eudatasharing.eu/homepage), which has been created by the Commission in order to put in place a series of measures facilitating voluntary data sharing, in particular by providing examples of good practices, standard contractual clauses or existing contract models (Commission Staff Working Document establishing a guidance on sharing private sector data in the European data economy accompanying the Communication '*Towards a common European data space*', Brussels, 25 April 2018, SWD(2018) 125 final, p. 6).

82 Recital 111 of the Data Act. Metzger and Schweitzer recommend to look for inspiration in the 'ALI/ELI Draft Principles for a Data Economy' (Wendehorst, C., & Cohen, N. (2021). ALI/ELI Principles for a Data Economy: Data Transactions and Data Rights, *ELI Final Council Draft*, <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf>) when drafting these model contract terms (Metzger, A., & Schweitzer, H. (2022). Shaping markets: A critical evaluation of the draft data act. *Available at SSRN 4222376*, p. 19).

83 Article 11 of the Data Act.

84 See Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157*, 15 June 2016.

85 Article 8.6 of the Data Act.

provision opens the door for the data holder to strategically claim the existence of trade secrets to refuse the sharing of the data'.[86] Others outline that Article 8.6 'arguably merely clarifies that the existence of the Data Act does not change the fact that the data is still subject to trade secret protection. It does not restrict the Data Act's data access claims'.[87] The final text of the Data Act further specifies how the balance between trade secret protection and the interest in stimulating data sharing should be struck. In particular, the Data Act now provides that a data holder can withhold or suspend data sharing based on a duly substantiated and written decision when the confidentiality of trade secrets is undermined.[88] Only in exceptional circumstances, the data holder may refuse on a case-by-case basis the request for access to the specific data in question when it can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets.[89] In both cases, the data holder has to notify the national competent authority. 'Serious economic damage' implies serious and irreparable economic losses. Based on objective elements, the data holder has to demonstrate 'the concrete risk of serious economic damage expected to result from a specific data disclosure and the reasons why the measures taken to safeguard the requested data are not sufficient'.[90] Such objective elements include 'the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product'.[91] Although it remains to be seen how these stipulations are applied in practice, they provide welcome guidance regarding the factors to be taken into account in assessing claims regarding trade secret protection. It is up to the national competent authorities (under the control of the courts) to develop decision-making practice on this issue. Worth mentioning is the explicit statement in the recitals that '[d]ata holders cannot, in principle, refuse a data access request under this Regulation solely on the basis that certain data is considered to be a trade secret, as this would subvert the intended effects of this Regulation'.[92] However, beyond this outer boundary, the provisions still leave significant room for interpretation.

86 Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), *op. cit.*, p. 102.

87 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit.*, p. 43.

88 Article 4(7) and 5(10) of the Data Act.

89 Article 4(8) and 5(11) of the Data Act.

90 Recital 31 of the Data Act.

91 Article 4(8) and 5(11) of the Data Act.

92 Recital 31 of the Data Act.

Second, the Data Act provides that the data holder may apply appropriate technical protection measures, including smart contracts,[93] to prevent unauthorised access to the data and to ensure compliance with the Data Act as well as with the agreed contractual terms.[94] Nevertheless, these technical protection measures may not be used to hinder the data sharing obligation.[95] In this regard, some argue that this provision should also 'further specify the technical requirements necessary to enable a legally compliant access and use'.[96] A key issue in this regard is that the Data Act 'does not specify in which format the data must be made accessible',[97] as this might significantly increase transaction costs. Accordingly, a fine line must be found between creating sufficient security and preserving the essence of the data sharing obligation.

Third, the data holder is protected against a data recipient's deceptive or abusive conduct. This covers situations like where the latter has provided inaccurate or false information to the data holder to obtain the data; deployed deceptive or coercive means or has abused evident gaps in the technical infrastructure of the data holder designed to protect the data; used the data for unauthorised purposes; or disclosed the data to another party without the data holder's authorisation.[98] Indeed, in such cases, the recipient must take several measures, including erasure of the data without undue delay, ending the production (or alike) of goods, derivative data or services produced on the basis of knowledge obtained through the data.[99] These seem reasonable requirements to protect data holders' interests.

93 "Smart contract' means a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering' (Article 2(39) of the Data Act). It is worth noting that the Data Act imposes five essential requirements (robustness and access control; safe termination and interruption; data archiving and continuity; access control; and consistency with the terms of the data sharing agreement) on vendors of smart contracts and on persons whose trade, business or profession involves the deployment of smart contracts for others in the context of data sharing agreements (Article 36 of the Data Act).

94 Article 11.1 of the Data Act.

95 Ibid.

96 Metzger, A., & Schweitzer, H. (2022). Shaping markets: A critical evaluation of the draft data act, *op. cit*., p. 23. For these authors, '[t]his gap is even more striking in light of the detailed provision on the technical requirements for interoperability in Article 28' (Ibid.)

97 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit*., p. 30. These authors suggest 'to include an obligation that data must be provided in a structured, common and machine-readable format or in a manner customary in the sector' (p. 31).

98 Article 11.3 of the Data Act.

99 Ibid.

2.3 Articulation with Personal Data Protection Considerations

We believe that an important gap in this horizontal framework is the lack of specific guidance regarding the interaction between data sharing obligations and the need to comply with the GDPR's personal data protection rules in situations where personal data have to be shared.[100] The Data Act states that it is without prejudice to the GDPR and that the GDPR prevails in cases of conflict.[101] One may therefore argue that this already clarifies the relationship between the two interests and that the legislator has set a hierarchy. However, in practice, such an approach is unlikely to be workable as many datasets targeted by the Data Act will include personal data and it will often not be clear at the outset to what extent any possible tension with the GDPR can be reconciled without putting the Data Act aside. Of course, the potential benefits that derive from data sharing are only acceptable if this is done in compliance with the rights of the individuals whose personal data could be shared.[102] However, because of the absence of more specific guidance on this issue in the Data Act itself, data holders might strategically invoke GDPR-compliance considerations to justify refusals to give effect to data sharing requests.[103]

A reason for the silence on this interaction with the GDPR in the Data Act may be that it is easier to strike a balance in each specific legislation imposing data sharing, as the compliance with the purpose limitation[104] and data minimisation[105] principles of the GDPR will be a function of the specific data covered and of the specific circumstances justifying the compulsory sharing. For instance, in the context of the IoT data access right, the Data Act provides that IoT generated personal data can only be shared with a third party if there is a valid legal basis under Article 6 or 9 of the GDPR.[106] In this regard,

100 On this point, see EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, p. 17-19; Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), *op. cit.*, p. 105-111.

101 Article 1(5) of the Data Act.

102 See European Data Protection Supervisor, *Opinion 3/2020 on the European strategy for data*, 16 June 2020, available at <https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf>, p. 8; Tombal, T. (2022). *Imposing Data Sharing among Private Actors*, *op. cit.*, p. 186-191 and 391-393.

103 Metzger, A., & Schweitzer, H. (2022). Shaping markets: A critical evaluation of the draft data act, *op. cit.*, p. 27.

104 Personal data can only be processed for specified, explicit and legitimate purposes, and cannot be further processed in a manner that is incompatible with those purposes (Article 5.1.b) of the GDPR).

105 Only the adequate, relevant and necessary data for the fulfilment of the specific purpose of processing shall be processed (Article 5.1.c) of the GDPR).

106 Articles 4.12 and 5.7 of the Data Act.

it is worth pointing out that the Data Act underlines that 'this Regulation does not create a legal basis for providing access to personal data or making personal data available to a third party'.[107] Another legal basis, such as consent or legitimate interests of the data controller,[108] thus has to be relied on. Importantly, according to the principle of separate justification, which provides that 'each transaction in data requires a legal basis at two levels: the level of the supplier of the data and the level of the recipient',[109] the third-party recipient will need its own legal basis for the further processing of this personal data.[110]

Regarding the IoT data access right, the Data Act also provides that third parties should only process the data 'for the purposes and under the conditions agreed with the user and subject to Union and national law on the protection of personal data including the rights of the data subject insofar as personal data are concerned', [111] and that they shall not use the data for profiling[112] purposes 'unless it is necessary to provide the service requested by the user'.[113] According to the EDPB and the EDPS, the Data Act should however explicitly remind all that any further personal data processing must comply with Article 6.4 of the GDPR, and should include clearer limitations or restrictions of reuse for 'purposes of direct marketing or advertising, employee monitoring, credit scoring or to determine eligibility to health insurance, to calculate or modify insurance premiums'.[114]

In light of the above, we believe that some overlapping principles are worth developing. An example could be a requirement to share, to the extent possible, anonymised data[115] rather than personal data – notably through resorting to the services of interme-

107 Recital 7 of the Data Act.

108 Respectively Articles 6.1.a) and 6.1.f) of the GDPR.

109 Wendehorst, C. (2017). Of elephants in the room and paper tigers: how to reconcile data protection and the data economy. In *Wendehorst, Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy, in Lohsse/Schulze/Staudenmayer (Eds), Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy* (Vol. 3, pp. 327-356), p. 334-337.

110 Tombal, T. (2022). *Imposing data sharing among private actors*, *op. cit*., p. 186.

111 Article 6.1 of the Data Act.

112 "Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements' (Article 4(4) of the GDPR).

113 Article 6.2.b) of the Data Act.

114 EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit*., p. 3 and 15-16.

115 The ISO 29100 standard defines anonymisation as the : 'process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party' (ISO 29100:2011, point 2.2, available at <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en>).

diary 'data trustees' charged with anonymising the data –[116] or a requirement to pseudonymise[117] the data where possible and to the extent that this does not affect reuse possibilities.[118] Moreover, the 'reasonable' compensation to be charged by the data holder to the data recipient could be interpreted as including the marginal costs of anonymising or pseudonymising the data.[119] It should also be recalled that if the recipient's further processing is not compatible with the data holder's initial processing, the recipient can only carry out the desired processing under the initial legal ground for processing if it has obtained the data subjects' consent or if this transfer is necessary to comply with a legal obligation.[120] In this regard, the specific purpose pursued will have to be outlined and only the data that are necessary to achieve this purpose can be shared with the recipient.[121] Finally, the data subjects should be clearly informed about this transfer in order to be able to exercise their rights.[122]

2.4 Dispute Resolution Mechanism

This horizontal framework for compulsory B2B data sharing is a welcome development as it aims to clarify upfront how to implement data sharing obligations, while trying to find a balance between the interests of both data holders and data recipients. However, by relying on data sharing agreements and by only limiting the data holder's contractual freedom to the extent necessary, it may inevitably cause delays to the data sharing process. Indeed, one can imagine that the data holder and the data recipient will not necessarily agree on what constitutes FRAND terms in their particular situation, and

116 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit*., p. 20.

117 Pseudonymisation is 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person' (Article 4.5 of the GDPR).

118 See, by analogy, Article 5.3 of the Data Governance Act. See also EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal, op. cit*., p. 14-15.

119 See, by analogy, Article 6.1 of Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information, *OJ L 172/56*, 26 June 2019.

120 Article 6.4 and Recital 50 of the GDPR. For more details, see De Terwangne, C. (2020). Principles relating to processing of personal data. In *The EU general data protection (GDPR): a commentary* (pp. 309-320). Oxford University Press, p. 309-320; Kotschy, W. (2020). Article 6 Lawfulness of processing. In Kuner, C. Bygrave, L. & Docksey, C. (eds.), *The EU General Data Protection Regulation (GDPR)*. Oxford University Press, Oxford, p. 321-344; European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union, 2018, p. 122-125.

121 Articles 5.1.b) and c) of the GDPR.

122 EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal, op. cit*., p. 14-15.

that this could lead to lengthy discussions slowing down the sharing process. This risk is in fact very real, as can be observed from the similar difficulties of determining what constitutes a FRAND licence in the context of standard essential patents (SEPs).[123] Some even argue that the potential for disputes will be higher for data licencing than for SEP licencing.[124]

To alleviate this potential issue, the Data Act establishes a dispute resolution mechanism that should offer 'a simple, fast and low-cost' solution to the parties.[125] More concretely, data holders and data recipients should have access to a dispute settlement body (DSB) that has been certified by the Member State in which it is established.[126] Such certification must be requested by the DSB, which will need to demonstrate that:

> (a) it is impartial and independent, and it is to issue its decisions in accordance with clear, non-discriminatory and fair rules of procedure;
>
> (b) it has the necessary expertise, in particular in relation to fair, reasonable and non-discriminatory terms and conditions, including compensation, and on making data available in a transparent manner, allowing the body to effectively determine those terms and conditions;
>
> (c) it is easily accessible through electronic communication technology;
>
> (d) it is capable of adopting its decisions in a swift, efficient and cost-effective manner in at least one official language of the Union.[127]

123 See, for instance, Geradin, D. (2013). Ten Years of DG Competition Effort to Provide Guidance on the Application of Competition Rules to the Licensing of Standard-Essential Patents: Where Do We Stand?. *Available at SSRN 2204359*., p. 7-8; Graham, C., & Morton, J. (2014). Latest EU Developments in Standards, Patents, and FRAND Licensing. *EURO. INTELL. PROP. REV.*, *36*, 700-705; Stern, R. H. (2015). What Are Reasonable and Non-Discriminatory Terms for Licensing a Standard-Essential Patent?. *Eur. Intell. Prop. Rev.*, *37*, 549-549; Drexl, J. (2017). Designing competitive markets for industrial data. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *8*, 257, *op. cit*., p. 55; ECJ, *Huawei*, 16 July 2015, C-170/13, EU:C:2015:477.

124 Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), *op. cit*., p. 38.

125 Article 10.1 and Recital 52 of the Data Act. Once again, the EDPB and the EDPS highlight that the data subject, whose data might be shared, is completely overlooked in this dispute resolution mechanism and that this may interfere with her right to lodge a complaint with a supervisory authority. (EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit*., p. 18).

126 Articles 10.1 and 10.5 of the Data Act.

127 Article 10.5 of the Data Act.

To make it easier for data holders and data recipients to identify these certified DSBs, the Member States will have to notify the Commission about the certified DSBs, so that they can be included in a list published and updated by the Commission on a dedicated website.[128]

With regard to the functioning of these DSBs, it is important to highlight that DSBs will have to reject requests to deal with disputes that have already been submitted to another DSB or to a Member State's court or tribunal to prevent multiple parallel procedures.[129] Moreover, parties will need to pay to resort to these procedures. However, the Data Act does not specify the amount of the fees nor a way to calculate them. It merely provides for a transparency requirement, namely that the DSB 'shall make the fees, or the mechanisms used to determine the fees, known to the parties concerned before those parties request a decision'.[130] The procedure itself should be adversarial, as both parties should be able to express their point of view on the issue and to answer to the other party's submissions as well as to any potential expert statements.[131] These debates will nevertheless have to occur within a short time span, as the DSB will have to decide on the matter maximum ninety days after receiving the request.[132] It thus resembles an arbitration by experts mechanism.

One might question whether this ninety-days deadline is realistic. On the one hand, the parties may file lengthy submissions and require numerous expert statements. On the other hand, the DSB's decision will have to contain a statement of reasons supporting its findings, which means that it will have to 'answer' to the parties' (potentially lengthy) submissions and to the (potentially numerous) expert statements.[133] All of this could take a substantial amount of time.

Moreover, the DSB's decision, which must be delivered in writing or through another durable medium, will only be binding on the parties if they 'have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings'.[134] Accordingly, an unwilling party (most likely a data holder unwilling to share data) can refuse to consent to the binding nature of this dispute mechanism. To be sure, a data recipient faced with an unwilling data holder retains its right to seek an effective remedy before Member States' courts or tribunals.[135] However, this will delay the dispute resolution, especially if the unwilling data holder drags its feet and is unwilling to cooperate. As a

128 Article 10.6 of the Data Act.
129 Article 10.7 of the Data Act.
130 Article 10.2 of the Data Act.
131 Article 10.8 of the Data Act.
132 Article 10.9 of the Data Act.
133 Ibid.
134 Articles 10.9 and 10.12 of the Data Act.
135 Article 10.13 of the Data Act.

result, while this speedy dispute resolution mechanism has been instituted in order to avoid lengthy discussions about the FRAND nature of the contractual terms, this will only work to the extent that both parties are willing to engage in such procedure and to agree to the binding nature of the decision. Otherwise, the dispute may have to be settled in court, which could take years, and this could hamper the development of innovative services by data recipients that need access to the data at hand.

In light of the above, it would have been welcome for the Data Act to make the DSB's decision binding on the parties.[136] Moreover, the Data Act could have made the dispute settlement mechanism a prerequisite to any FRAND-related procedure before national courts or tribunals. Indeed, the guarantees of independence, impartiality and expertise required to certify DSBs, as well as their duty to justify the reasons supporting their decision, should ensure the quality of their decisions, and should legitimate their binding nature. Moreover, providing that this speedy procedure is a prerequisite to a potential court case, this would have had the advantage of generating a first timely decision as to whether specific terms are FRAND. Overall, this could speed up the dispute resolution process and avoid unnecessary lengthy procedures that would hamper the core objective of the Data Act: enabling a wider use of data. It thus remains to be seen how effective the Data Act's dispute settlement mechanism will be in practice. More generally, this raises the question of appropriate enforcement, which we turn to now.

3. Enforcement

While the Data Act includes a chapter on implementation and enforcement (Chapter 9), the provisions leave quite some leeway and responsibility for Member States to set up the institutional frameworks in their territories. It should be noted that this discussion is to some extent separate from the discussion in section 2, which showed that private bargaining plays a large role in implementing the Data Act's baseline horizontal framework. At the same time, public enforcers remain ultimately responsible for interpreting and enforcing the different parts of the Data Act.

Two key aspects relating to enforcement will be discussed in this section: the competent authorities and the cross-border enforcement. Another relevant aspect that will not be covered here, but that is raised by others and therefore worth mentioning, is the uncertainty about whether private law remedies like injunctions and damages are available in case of breaches of the Data Act.[137]

136 See Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit.*, p. 46.

137 Podszun, R., & Offergeld, P. (2022). The EU data act and the access to secondary markets, *op. cit.*, p. 45; Leistner, M., & Antoine, L. (2022). IPR and the use of open data and data sharing initiatives by public and private actors. *Study commissioned by the European Parliament's Policy Department for*

3.1 Competent Authorities

The Data Act requires Member States to designate one or more competent authorities as responsible for enforcement, and it gives Member States the choice to rely on existing authorities or establish new ones.[138] While the provisions leave a large margin of discretion to Member States to select competent authorities, a couple of preconditions are set by the Data Act. First, national data protection authorities are responsible for monitoring the application of the Data Act as far as the protection of personal data is involved.[139] Second, the competence of sectoral authorities has to be respected for specific sectoral data exchange issues relating to the implementation of the Data Act.[140] Third, the competent authority responsible for the enforcement of the provisions regarding the switching of data processing services must have experience in data and electronic communication services.[141] Within these boundaries, Member States are free to allocate responsibility for enforcement to one or more authorities. When a Member State designates more than one competent authority, the Member State has to select a data coordinator to facilitate cooperation among the different competent authorities.[142]

The lack of more prescriptive requirements regarding the selection of competent authorities at the national level has advantages and disadvantages. The main advantage is that Member States have the opportunity to choose the arrangement that best fits their national circumstances. For instance, depending on the resources and staffing of the various national authorities, Member States may prefer designating their data protection authority as the only competent authority for enforcing the Data Act. Alternatively, they may decide to divide responsibility across the data protection and competition authority and grant the coordinating role to the authority that still has the most available space to take up additional tasks. Beyond the availability of resources, the selection of the competent authorities may also stem from a policy choice at the national level. This points at the main disadvantage of the discretion of Member States to designate competent authorities, namely that harmonisation of enforcement is at risk. Even though the provisions of the Data Act regulate the conditions of data access, the exper-

Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs, p. 118-119; Metzger, A., & Schweitzer, H. (2022). Shaping markets: A critical evaluation of the draft data act, *op. cit.*, p. 28-29; Drexl, J., Banda, C., Gonzalez Otero, B., Hoffmann, J., Kim, D., Kulhari, S.,... & Wiedemann, K. (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), *op. cit.*, p. 89-90.

138 Article 37.1 of the Data Act.

139 Article 37.3 of the Data Act.

140 Article 37.4.a) of the Data Act.

141 Article 37.4.b) of the Data Act.

142 Article 37.2 of the Data Act.

tise of the respective authority may influence its attitude towards enforcement. A data protection authority will likely prioritise the protection of personal data in implementing the data access right, while a competition authority may let the need for sharing and reuse of data prevail. Even though the Data Act states that it is without prejudice to the protection of personal data,[143] there are always borderline cases where the expertise of the respective authority is likely to determine whether it leans more towards keeping datasets closed to prevent privacy concerns or opening datasets up to stimulate further innovation. Member States can thus steer implementation by selecting the data coordinator. On the one hand, the designation of different competent authorities among Member States may give rise to useful experimentation and help to sharpen implementation over time. On the other hand, effective coordination among Member States may be a challenge if the data coordinators have different fields of expertise and work with different vocabularies.

Different preferences have already been expressed regarding the designation of competent authorities. The EDPB and the EDPS have asked the EU legislator to designate national data protection authorities as data coordinators under the Data Act.[144] According to the EDPB and the EDPS, data protection authorities have 'a unique expertise, both legal and technical … placing them at the core of the digital regulation landscape'.[145] In their view:

> the designation of coordinating competent authorities other than data protection authorities could affect consistency in terms of monitoring the application of the provisions of the GDPR and lead to real complexity for digital players and data subjects.[146]

However, one may wonder whether data protection authorities have the most suitable expertise to implement the Data Act's data access right. The EDPB and the EDPS stress the importance of the fundamental right to the protection of personal data,[147] while the Data Act mainly stems from the need to create competitive and innovative data markets. As noted by Leistner and Antoine,[148] competition authorities may therefore be more suitable as data coordinators than data protection authorities. Competition authorities have relevant experience involving, for instance, setting the conditions of access and

143 Recital 7 of the Data Act.
144 EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, par. 113.
145 EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, par. 114.
146 EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, par. 116.
147 EDPB-EDPS, *Joint Opinion 2/2022 on the Data Act Proposal*, *op. cit.*, par. 115.
148 M. Leistner and L. Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors', *op. cit.*, p. 72.

the determination of FRAND terms. To ensure that the data access right is implemented in a data protection-compliant way but also in a way that fits the Data Act's objectives to promote competitive and innovative data markets, a mix of expertise is required. It may therefore be sub-optimal to leave all responsibility for enforcement with data protection authorities, who are already involved in the monitoring of the Data Act to ensure the protection of personal data.

Accordingly, we recommend Member States designate competition authorities as the data coordinators, who will then have to liaise with data protection authorities for aspects involving personal data. While the text of the Data Act also leaves Member States the choice to set up a new authority, we believe this would unnecessarily risk duplicating resources and make the enforcement landscape at the national level even more complicated. Because effective cooperation between competition, data protection or other authorities will be key to ensure proper implementation of the Data Act, we suggest Member States put cooperation protocols in place describing how the competent authorities can exchange insights and involve each other's expertise in monitoring the application of the Data Act. Not every Member State may currently have effective cooperation mechanisms in place.

Beyond this, we recommend aligning the enforcement of the Data Act and the Data Governance Act by making the same national authority responsible for coordinating enforcement.[149] There are synergies between the two Acts. In particular, the Data Act's data access right can boost the development of data intermediaries, services which facilitate data sharing between data holders and data users,[150] for which the Data Governance Act has established a notification framework that is governed at the national level.[151] We submit that consolidation of enforcement within the same national authorities is desirable to reap the benefits of the synergies between the two Acts and to ensure a harmonised implementation of data access-related legal mechanisms.

3.2 Cross-Border Enforcement

A large part of the data processing that falls within the scope of the Data Act is likely not confined to a single Member State. For instance, manufacturers will typically offer IoT devices to users in different Member States in parallel, and third parties wishing to access data under the Data Act may be based in a different Member State than the manufacturer or user of the IoT device. In such cross-border situations, the entity is

149 See also Colangelo, G. (2022). European Proposal for a Data Act–A First Assessment. *CERRE Evaluation Paper*, *op. cit*., p. 29.

150 Article 2.11 of the Data Governance Act.

151 Article 10-12 of the Data Governance Act.

subject to the competence of the Member State in which it has its main establishment.[152] The same approach applies in the GDPR, where the national data protection authority of the main establishment of the undertaking concerned is automatically responsible for acting as lead supervisory authority.[153] The latter approach has led to enforcement bottlenecks in EU data protection law because big tech firms in particular have their main establishments in countries like Ireland and Luxemburg that struggle to take up cross-border cases because they require larger resources than their populations allow for.[154] It is therefore remarkable that the Data Act makes the same choice.

One alternative would have been to rely on the approach of cross-border enforcement within EU consumer law, according to which the competent authorities select the national consumer authority that is best placed to coordinate the case.[155] This allows for more flexibility to allocate cases of cross-border relevance to national authorities. This kind of mechanism also ensures that the available resources are more evenly spread across cross-border issues than is currently the case for the enforcement of the GDPR. Interestingly, the Data Act does let national competent authorities allocate cases on a first-come-first-served basis when dealing with entities that do not have an establishment in the EU, until they have appointed a legal representative in one of the Member States.[156] It remains to be seen whether the Data Act's choice to make the Member State of the main establishment competent will lead to a similar enforcement bottleneck as under the GDPR. What is clear is that the legislator's choice allows for strategic behaviour, whereby entities can consider which authority will be responsible for supervising their activities for the purposes of the Data Act when moving their main establishment or designating their legal representative.

4. Conclusion

The Data Act aims to address issues that slow down the development of the European data economy by creating a legal instrument to enable wider data use across the economy. To do so, the Act creates a baseline horizontal framework for compulsory data

152 Article 37.10 of the Data Act.

153 Article 56.1 of the GDPR.

154 Communication from the Commission to the European Parliament and the Council, '*Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation*', 24 June 2020, COM(2020) 264 final, p. 6; G. Gentile and O. Lynskey, 'Deficient by design? The transnational enforcement of the GDPR', *International & Comparative Law Quarterly*, 2022, Vol. 71, Issue 4, p. 799-830.

155 Article 17.2 of Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws (CPC Regulation), *OJ L 345/1*, 27 December 2017.

156 Article 37.11 and 13 of the Data Act.

sharing, which should provide incentives for horizontal data sharing across sectors. This is a truly novel approach compared to the previous disparate and mostly sector-specific data sharing approaches. Our analysis of the different provisions shows that it is possible to set conditions for data sharing that have a more general scope of application, but that there are several uncertainties in how they will be implemented. The success of the Data Act's horizontal framework for compulsory data sharing therefore largely depends on how its provisions are interpreted and applied. Several issues are worth keeping in mind in that process, including the need for guidance on what is 'reasonable' compensation for sharing data and on the interaction between data sharing obligations and the need to comply with personal data protection rules in situations where personal data have to be shared.

Despite the intention of the legislator to create clarity in the increasingly complex area of regulating data, it is important to highlight that the scope of the Data Act's horizontal framework is limited to compulsory B2B data sharing. This means that other legal frameworks will continue to exist for voluntary B2B data sharing, as well as for B2U, B2G, G2B and G2G data sharing. While this is due to the fact that different types of objectives are pursued depending on the type of data sharing, this might lead to an 'overload' of parallel data sharing regimes. This may hamper the fostering of data sharing more generally if there is no minimal alignment between the regimes.

The horizontal framework also only applies to the Data Act's IoT data access right and compulsory B2B data sharing obligations that enter into force after the date of application of the Data Act. Therefore, the horizontal framework does not apply to any pre-existing (sectoral) legislation that imposes compulsory B2B data sharing. In the short to medium term, this could lead to uncertainties for data holders due to the parallel application of different rules and regimes imposing compulsory B2B data sharing. It will thus be fundamental to ensure convergence between the Data Act's horizontal framework and these previously existing instruments in the coming years, possibly through anticipated revisions of these instruments if issues appear before their planned revision date. Similarly, as the Data Act provides that this is a baseline framework and that future legislation can go further in terms of data sharing requirements, it will be important to find the right balance between accommodating sector-specific needs on the one hand, and maintaining a minimum level of coherence between the different instruments on the other hand, in order to avoid a patchwork of data sharing regimes that would be hard to navigate.

Regarding enforcement, the Data Act leaves a lot of discretion to Member States to designate competent authorities and set up enforcement mechanisms. While the EDPB and the EDPS have advocated for designating national data protection authorities as coordinating competent authorities under the Data Act, competition authorities may possess more suitable expertise to take up this responsibility, considering the Data Act's

focus on promoting competitive and innovative data markets. To avoid the likely diversity of competent authorities designated by Member States from affecting the overall effectiveness of the enforcement system, we recommend Member States adopt cooperation protocols that describe how the different competent authorities can exchange insights and involve each other in monitoring compliance with the rules. Not every Member State will have this kind of cooperation protocol in place, while it is likely that authorities from different legal domains are involved in the application of the Data Act. Effective collaboration is thus vital to ensure proper implementation of the rules. Hopefully, the legislator's choice to make the Member State of the entity's main establishment competent for cross-border cases will still allow for a proper spread of responsibility across Member States and will not result in a similar enforcement bottleneck as in the GDPR.

To conclude, our analysis has illustrated the potential as well as the limits of the Data Act in creating a horizontal framework for data sharing. Its success in stimulating the data economy mainly depends on how ambiguities in the text are interpreted and what enforcement mechanisms are set up at the national level. As such, the Data Act forms an ambitious starting point for a next phase in the regulation of data sharing. While the Data Act's intention was to provide a clear and straightforward regime for data sharing, this chapter shows that many uncertainties are likely to remain in the coming years, at the very least until market players, regulators and courts start to find their way through the quagmire of different provisions and layers of regulation targeting data sharing in the EU.