EJLT European Journal of Law and Technology

The Influence of the Data Act on the Shifting Balance between Data Protection and the Free Movement of Data

Pieter T.J. Wolters[1]

Abstract

The relationship between data and European law is characterised by two objectives that need to be balanced: data protection and the free movement of data. This article analyses the influence of the Data Act on this balance. It argues that the Data Act will not significantly shift the balance by itself. Like the Data Governance Act, the Data Act primarily contains frameworks that apply when data are shared. However, the obligations and incentives to use these frameworks remain relatively limited. The strict rules of the GDPR are not affected.

This does not mean that the Data Act cannot play a meaningful role in the future. The Data Act is part of the broader European strategy for data. The extensive frameworks are not just meant for a few specific obligations to share data. They provide a foundation. It is up to other instruments, such as the European data spaces, to build on this foundation. The impact of the Data Act on the balance between data protection and the free movement of data is therefore not set in stone. It depends on the success and further elaboration and implementation of the European strategy for data.

Keywords: Data Act, data governance, data protection.

[1] Mr. Pieter T.J. Wolters is an associate professor of private law and a researcher at the Radboud Business Law Institute.

1. Introduction

On 19 February 2020, the European Commission announced the 'European strategy for data'.[2] This strategy aims to strengthen the free movement (or 'flow') of data. It aims to better capture the benefits of data and make them available to all.[3] An important pillar of this strategy is the Data Act.[4] After the Data Act proposal in February 2022, the European Parliament and the Council adopted their amendments and mandate in March 2023.[5] The final version was published on 13 December 2023. Like the European strategy for data, the Data Act has the objective of removing barriers to a well-functioning internal market for data. For this reason, it lays down harmonised rules for sharing data.[6]

Data-sharing is not without risks. Without adequate safeguards, it could negatively affect the protection of personal data. For this reason, the European strategy for data and the Data Act emphasise that data-sharing should be done in accordance with data protection law.[7] However, this does not guarantee that the new rules do not affect the protection of personal data. By their very nature, new possibilities to share data lead to new risks (Section 2). This leads to a shift in the balance between data protection and the free movement of data. In recent years, the emphasis has been on data protection (Section 3). A strict interpretation of data protection law has made it harder to share data. The European strategy for data and the Data Act attempt to move the centre of gravity in the other direction.

In this article, I examine this shifting balance. Through a close reading of the various provisions of the Data Act, I analyse how this Regulation affects this balance. In this light, the primary objective of this article is to better understand how the Data Act navigates this tension between the various objectives and whether it reaches its

---

[2] Commission, 'A European strategy for data' (Communication) COM(2020) 66 final. See also Commission, 'Shaping Europe's digital future' (Communication) COM(2020) 67 final, 7–10.

[3] Ibid 1–3, 6–8; Giovanni Comandè and Giulia Schneider, 'It's time: Leveraging the GDPR to shift the balance towards research-friendly EU data spaces' (2022) 59 *Common Market Law Review* 739, 739–740, 759–760. See also n 6.

[4] 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) [2023] OJ L2023/2854.

[5] 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; European Parliament, 'Amendments adopted by the European Parliament on 14 March 2023 on the 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)' P9_TA(2023)0069; Council, '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) – Mandate for negotiations with the European Parliament' 7413/23.

[6] About the objectives of the Data Act, see Data Act, art 1(1), recitals 1–4; Data Act proposal (n 5) 1–3, 6–7; 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 to and use of data (Data Act)' (Staff Working Document) SWD(2022) 34 final, 1–3, 7–28.

[7] Commission, 'A European strategy for data' (n 2) 1, 5, 22; Data Act, art 1(5), recitals 7–8, 35, 102.

goals. However, I will also critically reflect on the various choices that have been made. The focus is on the Data Act, but this regulation is also analysed in the context of broader developments. I answer the following research question: *How does the Data Act affect the balance between data protection and the free movement of data?*

The article begins with a general description of the relationship between European law and data. The research question could imply that data protection and the free movement of data are always opposing objectives. This is not the case. As Section 2 explains, the free movement of data and data protection are often intertwined. This is followed by a brief description of data protection law and its strict interpretation (Section 3). I subsequently elaborate on how the European strategy for data (Section 4) and the Data Act (Section 5) change the *status quo*. I conclude (Section 6) that the Data Act does not *by itself* significantly affect the balance between data protection and the free movement of data. Its impact ultimately depends on the success and further elaboration and implementation of the European strategy for data.

2. The Dual Objective in the Relationship between Data and European Law

The relationship between data and European law cannot be separated from the general objectives of the European Union. Pursuant to Article 3(3) TEU, one of the objectives of the European Union is to create an internal market. The free movement of data is a part of this market. It requires that data can be used and shared throughout the European Union. This should not be limited by legal fragmentation or national localisation requirements.[8]

The free movement of data has held the special interest of the European Commission since 2015.[9] In that year, the Commission presented its Digital Single Market strategy. This strategy is aimed at a better utilisation of the potential of digitalisation.[10] The removal of legal barriers for the use and sharing of data is one of its components.[11]

Since 2015, the European Union has adopted several instruments to strengthen the free movement of data. Notably, the General Data Protection Regulation (GDPR) is partly intended to harmonise data protection law and thereby ensure the free movement of personal data,[12] the 'Free Flow of Non-personal Data Regulation'

[8] In the context of the various instruments, see nn 3, 11, 12, 13, 14, 15, 45, 46. See also J.A. Hofman, *De beveiliging van persoonsgegevens. Over de juridische invulling van art. 5 lid 1 onder f en 32 AVG* (Wolters Kluwer 2022) 195–199; Comandè and Schneider (n 3) 745.

[9] See also Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca, *The Evolution of EU Law* (OUP 2021) 905–906, 919–920 for an overview of older developments.

[10] Commission, 'A Digital Single Market Strategy for Europe' (communication) COM(2015) 192 final, 3–4.

[11] Ibid 14–15.

[12] Regulation 2016/679/EU 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 [2016] OJ L119/1, art 1, recital 2, 3, 6, 7, 9, 10, 11, 13, 53, 123, 166, 170;

prohibits 'data localisation requirements' for non-personal data[13] and the 'Open Data Directive' contains rules about the access to documents of public sector bodies and public undertakings.[14] Finally, access to certain data such as account information and data about electricity use has been reinforced by sector-specific instruments such as the PSD2 and the 'Electricity Directive'.[15]

Strengthening the internal market is not the only relevant objective of the European Union. Pursuant to Articles 2 and 3(1) TEU, it also has the aim of promoting human rights and other important values. This includes the protection of personal data.[16] The Digital Single Market strategy[17] and the various European instruments therefore consistently emphasise that the free movement of data should be accompanied by an adequate protection of personal data.[18]

The relationship between data and European law is thus characterised by a 'dual' objective:[19] (1) it should be possible to share and use data within the European Union; but (2) this should not negatively affect the protection of personal data. There is a clear tension between these objectives. European rules are typically designed to

---

Viviane Reding, 'The European data protection framework for the twenty-first century' (2012) 2 *IDPL* 119, 121; Bart van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 *IDPL* 307, 317; Simon Davies, 'The Data Protection Regulation: A triumph of Pragmatism over Principle?' (2016) 2 *EDPL* 290, 293–294; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *CLSR* 179, 182; P.T.J. Wolters, 'The security of personal data under the GDPR: a harmonized duty or a shared responsibility?' (2017) 7 *IDPL* 165, 165–166; Hofman (n 8) 197–199; Laura Drechsler, 'Did the Court of Justice (re-)define the purpose of the General Data Protection Regulation?' (KU Leuven CiTiP 14 February 2023) <https://www.law.kuleuven.be/citip/blog/did-the-court-of-justice-re-define-the-purpose-of-the-general-data-protection-regulation/> accessed 26 January 2024. See also n 26.

[13] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59, arts 3(1), (5), 4(1). About the objectives of this Regulation, see art 1, recitals 4, 10, 13, 18, 20, 39.

[14] Directive (EU) 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 [2019] OJ L172/56, arts 1(1), 2(1), (3), (6), recitals 13, 17, 18, 59, 68, 70.

[15] About the PSD2, see 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 [2015] OJ L337/35; P.T.J. Wolters and B.P.F. Jacobs, 'The security of access to accounts under the PSD2' (2019) 35 *CLSR* 29. About the Electricity Directive, see 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 [2019] OJ L158/125, art 3(4), 23(2). See Commission, 'A European strategy for data' (n 2) 4 for more examples.

[16] See also TFEU, art 16; Charter EU, art 8.

[17] Commission (n 10) 3, 9, 13. See also n 7.

[18] See e.g. GDPR, art 1, recitals 1, 6, 7, 10, 11; Free Flow of Non-personal Data Regulation, arts 2(2), 3(1), 8(3), recitals 8, 9, 37; Open Data Directive, arts 1(4), recitals 16, 28, 44, 52, 53, 71; PSD2, art 94; Electricity Directive, art 23(3).

[19] E.g. Hofman (n 8) 204–211; Streinz (n 9) 910; Drechsler (n 12) ('double-headed').

promote both objectives. However, it should be emphasised that these objectives are not always at odds. European rules are often designed to promote both objectives. Most notably, as mentioned above, the GDPR is intended to strengthen both the free movement of data and data protection. Stronger data protection law can also facilitate the free movement of data.[20] More generally, the data protection risks of data-sharing can be reduced with safeguards. In these situations, the free movement of data can be strengthened without substantial negative effects on data protection. At the same time, such safeguards cannot remove the tension altogether. The (removal of legal barriers for the) use and sharing of personal data inherently leads to new risks of misuse and data breaches. It is therefore necessary to balance the two objectives. Any limitation of the fundamental right to data protection should be proportional and respect the essence of this right.[21]

3. Data Protection Law

The core of the European data protection law is formed by the GDPR. Other relevant instruments include the 'Law Enforcement Directive', the 'ePrivacy Directive' and the Charter of Fundamental Rights of the European Union.[22] The GDPR applies to the 'processing' of the 'personal data' of 'data subjects'.[23] Any operation performed on personal data is a 'processing'. This includes sharing the data. 'Personal data' means *any* information relating to an identified or identifiable natural person (the 'data subject'). The obligations of the GDPR are imposed on the natural or legal persons that process the personal data: the 'controller' and the 'processor'.[24]

Several obligations of the GDPR are relevant for data-sharing. For example, the principle of 'data minimisation' in Article 5(1)(c) GDPR requires that personal data are

[20] N 12. See also in the context of the rights of data subjects GDPR, recitals 7, 68; Wolters (n 12) 165–166; P.T.J. Wolters, 'The Control by and Rights of the Data Subject Under the GDPR' (2018) 22 *Journal of Internet Law* 1, 1, 10; Hofman (n 8) 202–204.

[21] Charter EU, art 52; Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 60; Hofman (n 8) 158–177; Streinz (n 9) 934; Gloria González Fuster, *Study on the essence of the fundamental rights to privacy and to protection of personal data* (EDPS 2021/0932, 2022); Plixavra Vogiatzoglou and Peggy Valcke, 'Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law' in Eleni Kosta, Ronald Leenes and Irene Kamara (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar 2022) 33–40.

[22] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, last amended by Directive 2009/136/EC; Charter of Fundamental Rights of the European Union (OJ C326/391). The European Commission has proposed an ePrivacy Regulation in 2017. See n 91.

[23] GDPR, arts 2(1), 4(1)–(2).

[24] GDPR, art 4(7)–(8).

only shared when necessary in relation to the purposes for which they are processed. Furthermore, sharing data is only lawful if the controller can invoke one of the grounds of Article 6(1) GDPR, such as consent or necessity for a contract. Sharing data with a processor is only allowed if the receiver provides the necessary data protection safeguards.[25] Finally, sharing data with receivers outside the European Union is only permissible under certain conditions pursuant to Chapter V GDPR.

In recent years the GDPR has consistently been interpreted in a strict way by the Court of Justice and the European Data Protection Board (EDPB).[26] This makes it more difficult to share data.[27] In this section, I give some examples of these interpretations.

Most importantly, the concepts of 'identifiable' and 'personal data' are interpreted broadly. They are not limited to information with a strong connection to a person[28] or situations in which the data subject is identified by a name or other unique characteristic (address, e-mail address, personal or employee number). Instead, it is argued that a data subject could already be identifiable if it can be distinguished or 'singled out' within a group.[29] Consequently, data should not be easily considered anonymised, and therefore not 'personal'.[30] The GDPR thus almost always applies to sharing data, even if the connection of a dataset to natural persons appears to be absent at first sight.[31]

---

[25] GDPR, art 28.

[26] See also Hofman (n 8) 206–211; Drechsler (n 12).

[27] See also e.g. Comandè and Schneider (n 3) 746, with references to further literature. See also n 31, 52.

[28] Cf Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection' (2018) 10 *Law, Innovation and Technology* 40, 45.

[29] About this discussion, see Case C-582/14 *Breyer* [2016] ECLI:EU:C:2016:779; Case T-557/20 *SRB v EDPS* [2023] ECLI:EU:T:2023:219; Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (01248/07/EN WP 136, 2007) 12–13; Article 29 Data Protection Working Party, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising* (02005/11/EN WP 188, 2011) 8; Article 29 Data Protection Working Party, *Appendix. Core topics in the view of trilogue* (17 June 2015) 5 (adding that singling out allows the date subject to be treated differently); Frederik J. Zuiderveen Borgesius, 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation' (2016) 32 *CLSR* 256, 265–270; Nadezhda Purtova, 'From knowing by name to targeting: the meaning of identification under the GDPR' (2022) 12 *IDPL* 163, 165–166, 181–182.

[30] Article 29 Data Protection Working Party (n 29) 21; Zuiderveen Borgesius (n 29) 262–264; Michèle Finck and Frank Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' (2020) 10 *IDPL* 11; Streinz (n 9) 916–917.

[31] E.g. Raphaël Gellert and Inge Graef, 'The European Commision's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing' in P.T.J. Wolters and others (eds), *Digitalisering en conflictoplossing* (Wolters Kluwer 2021) 224; Comandè and Schneider (n 3) 741–743; Streinz (n 9) 916–917.

The strict interpretations also concern the grounds for the lawfulness of a processing.[32] First, the necessity for a contract (Article 6(1)(b) GDPR) can only be invoked for a processing that is 'objectively' indispensable for a purpose that is 'integral' to the contractual obligation.[33] For example, it does not provide a ground for sharing data[34] in order to personalise advertisements in a free online service.[35]

Second, the service providers cannot make access to the service dependent on the data subject's consent (Article 6(1)(a) GDPR). Refusing consent would otherwise lead to negative consequences for the data subject, which is not allowed.[36] More generally, a controller may not abuse its dominant position in order to obtain consent for the sharing of data or any other processing that is not strictly necessary for the performance of the contract.[37] It is also not allowed to entice data subjects to give consent through deceptive design choices. Consent should be specific, informed and unambiguous pursuant to Article 4(11) GDPR. If a controller asks for consent, for example through a 'cookie banner', refusing should not be more difficult than consenting.[38] In any case, a pre-checked checkbox will not result in valid consent.[39]

Finally, the ground of legitimate interest (Article 6(1)(f) GDPR) also contains restrictions. Although data-sharing could further a legitimate interest, it is only allowed if the processing is necessary in order to achieve that interest, and the rights of the data subjects do not override that interest. Although it may be possible to share data with specific recipients for specific important purposes, extensive data-sharing

[32] See generally Case C-251/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 93. See also Michael Veale, Midas Nouwens and Christiana Teixeira Santos, 'Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?' [2022] *Technology and Regulation* 12.

[33] Case C-251/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, paras 98–99. See also EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0* (2019) 9–10 ('objectively' necessary for the 'fundamental objective' of the contract).

[34] For an illustration of the importance of data-sharing for personalised advertisements and the lack of a legal ground, see the Belgium Litigation Chamber of the Data Protection Authority 2 February 2022, Case number DOS-2019-01377, *IAB Europe*.

[35] Case C-251/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 102; EDPB (n 33) 14–16.

[36] GDPR, arts 4(11), 7(4), recital 42; Case C-251/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 150; EDPB, *Guidelines on Consent under Regulation 2016/679. Version 1.1* (2020) 7–8, 12–13.

[37] GDPR, recital 43; Case C-251/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 149.

[38] 'Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation' <www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance> accessed 5 July 2023; EDPB, *Report of the work undertaken by the Cookie Banner Taskforce* (2023) 5–6. This issue is governed by the ePrivacy Directive, which refers to the Data Protection Directive (the predecessor of the GDPR) for the definition of consent.

[39] Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801.

for online advertising or a wide variety of undefined purposes will generally not pass this balancing test.[40]

The rules on sharing personal data with persons outside of the European Union ('transfers') are also interpreted in a strict way. First, the application of these rules is not limited to situations in which the data are sent to a server outside the European Union. Remote access from a third country to data that are stored in the European Union also constitutes a 'transfer'.[41] Furthermore, transfers are only allowed if the level of protection is not undermined.[42] 'Not undermined' can be interpreted 'holistically' or 'risk based': a somewhat lower level of protection could suffice if the risks are limited.[43] However, the Court of Justice and (more explicitly) the Austrian supervisory authority rejected this approach and opted for a stricter interpretation.[44]

Taken together, these interpretations severely complicate data-sharing. The broad interpretation of 'personal data' means that the GDPR will almost always apply whereas the strict interpretations of the grounds for processing and data transfers limit the possibilities to use and share personal data.

---

[40] Cf Belgium Litigation Chamber of the Data Protection Authority 2 February 2022, Case number DOS-2019-01377, *IAB Europe*, paras 423, 442; Case C-251/21 *Meta v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, paras 116–118.

[41] EDPB, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (2021) example 5; Xavier Tracol, '"Schrems II": The return of the Privacy Shield' (2020) 39 *CLSR* 105484, 9, 11.

[42] E.g. GDPR, art 44, recital 104; Case C-362/14 *Schrems I* [2015] ECLI:EU:C:2015:650; Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559; Article 29 Data Protection Working Party, *Adequacy Referential* (18/EN WP 254 rev.01, 2018) chapter 1; EDPB, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (2021) 3; EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0* (2021) 9.

[43] Paul Roth, 'Adequate level of data protection' in third countries post-*Schrems* and under the *General Data Protection Regulation*' (2017) 25 *Journal of Law, Information and Science* 49, 60–62; Joshua P. Meltzer, 'The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security' (*Brookings* 5 August 2020) <https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/> accessed 2 December 2022. Oliver Patel and Nathan Lea, 'EU–U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows' (UCL European Institute Policy Paper 2020) 9–10; Laura Bradford, Mateo Aboy and Kathleen Liddell, 'Standard contractual clauses for cross-border transfers of health data after *Schrems II*' (2021) 8 *Journal of Law and the Biosciences* 1, 14; Paul Breitbarth, 'A Risk-Based Approach to International Data Transfers' [2021] *EDPL* 539, 548–549.

[44] Case C-311/18 *Schrems II* [2020] ECLI:EU:C:2020:559; DSB, *Datenschutzbeschwerde (Art. 77 Abs. 1 DSGVO). […], vertreten durch NOYB/1. […] und 2. Google LLC* (22 April 2022) <https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt.pdf> accessed 2 December 2022; Meltzer (n 43); Bradford, Aboy and Liddell (n 43) 14; Lokke Moerel, 'What happened to the risk-based approach to data transfers?' (Future of Privacy Forum 27 September 2022) <https://fpf.org/blog/what-happened-to-the-risk-based-approach-to-data-transfers/> accessed 2 December 2022.

4. The European Strategy for Data

The previous sections demonstrate a difference in emphasis. The *European Commission* has been particularly concerned with the free movement of data (Section 2). However, the strict interpretation of the GDPR by the *Court of Justice* and the *EDPB* has restricted the possibilities to share data in favour of stronger data protection (Section 3).

In this light, it is no surprise that the European Commission's European strategy for data focuses on strengthening the free movement of data.[45] The strategy thus builds on the Digital Single Market strategy, but places different emphases. The legal instruments of the Digital Single Market strategy are primarily aimed at the *creation* of a digital single market. They remove legal barriers to move or share data between the various Member States of the European Union.[46] The European strategy for data focusses more strongly facilitating and encouraging the sharing and use of data *within* this digital single market. At the same time, this strategy also emphasises that fundamental rights should be protected.[47] The dual objective is not compromised.

The European strategy for data identifies problems related to fragmentation between Member States, data-sharing in 'government-to-business' (G2B), B2G, B2B and G2G relationships, imbalances in market power, data interoperability and quality, 'data governance', data infrastructure, the exercise of rights by individuals, data literacy and cybersecurity.[48] The strategy seeks to solve these problems through measures based on four pillars: a cross-sectoral governance framework for data access and use; investments in data and infrastructure; investments in skills and SMEs; and common European data spaces in strategic sectors and domains of public interest.[49]

The European strategy for data has already led to (proposals for) legal instruments. Apart from the Data Act, the Data Governance Act (DGA) is the most notable. This Regulation was adopted on 30 May 2022 and applies from 24 September 2023. It creates conditions or frameworks for 'data intermediation services', 'data altruism' and the re-use of 'data' held by 'public sector bodies'.[50] However, the DGA does not

[45] Streinz (n 9) 934; n 3. See also European Council, 'Special meeting of the European Council (1 and 2 October 2020) – Conclusions' (2020) EUCO 13/20, 5; European Parliament, 'European strategy for data' (resolution) P9_TA(2021)0098; European Council, 'Statement of the Members of the European Council' (2021) SN 18/21, 4; European Council, 'European Council meeting (21 and 22 October 2021) – Conclusions' (2021), EUCO 17/21, 2; Data Act proposal (n 5) 1–3; Impact Assessment (n 6) 1–3. Note that this focus should not be understood as a direct reaction to the strict interpretations discussed in Section 3. See already in 2017, Commission, 'Building a European data economy' COM(2017) 9 final.

[46] N 11. Cf Impact Assessment (n 6) 3.

[47] N 7.

[48] Commission, 'A European strategy for data' (n 2) 6–11.

[49] Ibid 11–23. See Section 5.3 ondata spaces.

[50] 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) (2022) OJ L152/1, arts 1(1), 2(1), (10), (11), (16), (17).

create any new rights or obligations to share data.[51] Moreover, it does not contain rules that make it easier to share data as a data intermediation service or data altruism organisation. The application of the GDPR to data-sharing is unaffected. The strict interpretation of this Regulation, and especially of the concept of 'personal data', means that these rules apply to almost every dataset (Section 3). It therefore remains to be seen to what extent these data intermediation services and data altruism organisations will really play a significant role.[52]

5. The Data Act

The previous sections demonstrate that the Data Act is part of a long line of European instruments that seek to strengthen the free movement of data. In this section, I describe how the Data Act contributes to this goal and how it aligns with the earlier instruments.

The Data Act covers diverse and heterogeneous topics. Like the DGA (Section 4), it primarily imposes general (Section 5.1) and specific (Sections 5.2 and 5.3) legal *frameworks* for data-sharing. However, the Data Act also contains *rights* of access to data, in particular for users (Section 5.4) and public sector bodies (Section 5.5). In all cases, the concept of 'data' is defined broadly. Pursuant to Article 2(1), it refers to 'any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording'. It includes both personal and non-personal data.[53]

5.1 General Frameworks for Data-Sharing

Chapters III and IV Data Act impose legal frameworks for data-sharing. The scope of these frameworks is much broader than the more specific DGA (Section 4). Chapter III applies to business-to-business relations in which a 'data holder' (see Section 5.4.2) is obligated to make data available in pursuant to Article 5 Data Act or other Union law or its national implementations.[54]

Article 8(1) Data Act states that the data holder shall share the data under fair, reasonable and non-discriminatory terms, and in a transparent manner. These terms should be laid down in a contractual agreement with the data recipient.[55] The data

[51] See explicitly DGA, art 1(2).
[52] Gellert and Graef (n 31) 234, 239; Corina Kruesz and Felix Zopf, 'The Concept of Data Altruism of the draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU' [2021] *EDPL* 569, 579; Winfried Veil, *Data Altruism: how the EU is screwing up a good idea* (AlgorithmWatch 2021) 6–7; Gabriele Carovano and Michèle Finck, 'Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy' (2023) 50 *CLSR* 105830, 10–12. Cf Comandè and Schneider (n 3) 764–768.
[53] N 103.
[54] Data Act, arts 8(1), 12(1).
[55] See also Data Act, art 2(14), recital 42. This obligation was added by the European Parliament. Cf Data Act proposal (n 5), art 8(1); Amendments (n 5), art 8(1).

holder may charge a fee for making data available, even if it is obliged to share the data. However, this fee must be non-discriminatory and reasonable.[56] Furthermore, data holders and data recipients shall have access to certified dispute settlement bodies if there is a conflict in relation to the terms.[57]

Chapter IV applies to contractual terms concerning the access to and use of data in business-to-business relations, even if such access or use is not based on a legal obligation. Article 13(1) Data Act states that 'unfair' terms are 'not binding' if they are 'unilaterally imposed'. If the unfair term is severable from the remaining terms of the contract, those remaining terms remain binding pursuant to Article 13(7). Finally, the provision does not apply to contractual terms that define the price or main subject matter of the contract pursuant to Article 13(8). This provision of the Data Act bears clear similarities to the regulation of unfair terms in consumer contracts.[58] However, the exact requirements are different.

Pursuant to Article 13(3) Data Act, a contractual term is unfair if its use grossly deviates from good commercial practice and is contrary to good faith and fair dealing. This is further fleshed out with examples of terms that are always (Article 13(4)) or presumed ((Article 13(5)) unfair.[59] Under Article 13(6), a term is unilaterally imposed if it has been supplied by one party and the other contracting party has not been able to influence its content *despite* an attempt to negotiate it. Article 13 thus does not apply to terms that are accepted without an attempt at negotiation or to terms that are amended after negotiations.[60] Interestingly, Article 13 does not distinguish on the basis of whether the term was supplied by the data holder or the data recipient. It should thus apply to both situations. On the other hand, recital 58 shows that the Data Act is primarily concerned with the situation in which the data recipient is confronted with unilaterally imposed terms. In this light, the provision complements Article 8(1). Whereas Article 8(1) *obligates* the *data holder* to enter into a contractual agreement, Article 13 *stimulates* the *data recipient* to negotiate the proposed terms. Taken together, both provisions stimulate the parties to make clear and fair contractual agreements.

Chapters III and IV are designed to ensure that data-sharing is done on fair terms. However, it should be stressed again (Section 4) that these rules are only relevant if the data are shared. The chapters do not create any new rights or obligations to share

[56] Data Act, art 9(1). See also Data Act, art 9(6), recital 46.
[57] Data Act, art 10.
[58] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.
[59] Cf Directive 93/13/EEC, which only provides an annex of terms that *may be regarded* as unfair pursuant to Article 3(3). However, many Member States have implemented lists of terms that are always or presumed unfair. See Christian von Bar and Eric Clive (eds), *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR). Full Edition. Volume I* (OUP 2010) 662–667.
[60] Data Act, recital 59.

data or address the most pressing legal obstacles. They will thus not significantly strengthen the free movement of data by themselves.

5.2 Preventing 'Vendor Lock-in' and other Rules for 'Data Processing Services'

In addition to the broadly applicable frameworks discussed in Section 5.1, the Data Act also contains several more specific rules. First, it contains a special framework for 'data processing services'. This concept specifically refers to cloud services.[61]

Chapter VI Data Act creates a specific right to 'data portability' (see also Section 5.4.2) in order to solve the problem of 'vendor lock-in'.[62] Contractual, technical and economic factors can make it difficult to transfer data to another provider. Article 23 Data Act therefore obligates the providers to ensure that their customers can switch to another data processing service of the same type. In contrast to the frameworks discussed in Section 5.1, this right applies to both professional customers and consumers.[63] It is not entirely new. The obligations in the Data Act complement the codes of conduct that have been established pursuant to the Free Flow of Non-personal Data Regulation. However, this self-regulatory approach did not sufficiently eliminate the problem.[64]

Under the Data Act, customers must be able to switch to another provider or to port all their data, applications and digital assets to an on-premise ICT infrastructure within a transition period of no more than 30 calendar days. They have a right to retrieve their data for at least another 30 days.[65] The rights and obligations in relation to switching between providers must be clearly set out in a written contract pursuant to Article 25 Data Act. Again (see Section 5.1), the Data Act does not only impose fair terms: it also creates an obligation to clearly stipulate these terms in a contract.

The other provisions of the framework for data processing services aim to make the process of switching easier and more transparent. They deal with information obligations (Articles 26 and 28), the obligation to collaborate in good faith (Article 27), the gradual withdrawal of switching charges (Article 29), technical aspects (Article

[61] Data Act, art 2(8), recitals 78, 80, 96, 99, 100, 102. Recitals 78 and 102 also mention 'edge services' as an example of a data processing service.

[62] About this problem see e.g. Justice Opara-Martins, Reza Sahandi and Feng Tian, 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective' (2016) 5 *Journal of Cloud Computing: Advances, Systems and Applications*; Ron Davies, *Cloud computing. An overview of economic and policy issues* (In-Depth Analysis for the European Parliament, PE 583.786); Douglas Hayward and others, *Switching of Cloud Services Providers* (Study for the European Commission) 3–4; Impact Assessment (n 6) 5, 9, 14–15, 27.

[63] Cf Data Act, art 2(30), which defines 'customer' as a natural or legal person.

[64] Free Flow of Non-personal Data Regulation, art 6(1)(a); Data Act, art 1(7); Data Act proposal (n 5) 4; Impact Assessment (n 6) 4, 57. See also Section 5.4.2 on the right to data portability of the user.

[65] Data Act, art 25(2)(a), (g).

30), interoperability (Articles 34 and 35; see also Section 5.3) and certain exceptions for tailor-made and testing services (Article 31).

The framework also contains safeguards. Article 32 Data Act obligates data processing service providers to take all adequate technical, legal and organisational measures to prevent prohibited international transfers of or government access to non-personal data. This may apply, for example, to data pertaining to national security or defence, but also to trade secrets, intellectual property rights or other commercially sensitive data.[66] 'International' should be understood with reference to the free movement of data within the digital single market (see Section 2). It only refers to 'third' countries outside of the European Union.[67] This provision for *non*-personal data thus complements the rules on the transfers of *personal* data discussed in Section 3. The existence of these and other data protection rules also explains why Chapter VI of the Data Act does not contain specific safeguards in relation to data protection. The switching between data processing service providers does not lead to meaningful additional risks, and the customer and both the new and old provider have to apply with all relevant provisions of the GDPR.

The specific rules for data processing services differ from the more general provisions discussed so far. They do not only create legal frameworks that apply *if* data are shared, but also create a specific right to data portability. They thus actually impose an obligation to transfer data to another provider. Although safeguards do exist, the core of the new specific right to data portability remains unaffected. The provisions thus strengthen the free movement of data. At the same time, the specific nature of this right means that its influence is limited to the relation between the provider and the customer of a data processing service. In contrast, the strict interpretations of the GDPR concern its core concepts and rules (Section 3). For this reason, the specific right to data portability does not fundamentally alter the balance between data protection and the free movement of data in European law by itself.

5.3 Specific Frameworks for 'Smart Contracts' and 'Data Spaces'

The final specific legal frameworks included in the Data Act deal with 'smart contracts' and 'data spaces'. Pursuant to Article 2(39), a 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'. The requirements set out in Article 36 Data Act focus on the security and availability of smart contracts that are used to execute an agreement to make data available. Again (see Section 5.1), these requirements only apply if smart contracts are used for this purpose. They do not create any rights or obligations to share data themselves.

[66] Data Act, recital 101.
[67] See also Data Act, art 32(2)–(3), recital 101.

Article 33 Data Act formulates essential requirements for participants in data spaces. These requirements focus on interoperability: 'the ability of two or more data spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions'.[68] The concept of 'data spaces' is not defined in the Data Act, but can be derived from the European strategy for data. Pillar D of this strategy envisions the establishment of a total of nine common European data spaces in strategic sectors and domains of public interest.[69] Like the rest of the strategy, these data spaces are intended to strengthen the free movement of data. However, the strategy does not clarify whether, and to what extent, this involves legal obligations to share data. The measures listed in the appendix mainly concern frameworks.[70] The first proposal, for a 'European Health Data Space', provides more clarity. It contains provisions on the frameworks and infrastructure for sharing health data, but also creates rights of access in relation to 'electronic health data' for natural persons to whom these data relate, for 'health professionals' and for 'secondary use'.[71]

The rules on data spaces thus illustrate how the frameworks in the DGA and the Data Act are a part of the broader European strategy for data. The DGA and the Data Act primarily (but not exclusively; see also Sections 5.2, 5.4 and 5.5) create legal frameworks. They provide a foundation. Other instruments, such as the European data spaces, can subsequently build on this foundation. They could ensure the use of the frameworks by creating rights and obligations to share data.

5.4 The Access of the User

5.4.1 The Scope of the Rights

The Articles 3, 4 and 5 Data Act create rights for the 'user' of 'connected products' and 'related services'. First, the 'user' is a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.[72] It can either be a business or a consumer.[73]

Pursuant to Article 2(5), 'connected product' refers to an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access.[74] The concept is specifically meant for products that are connected to

[68] Data Act, art 2(40). See also Data Act, arts 34, 35.
[69] Commission, 'A European strategy for data' (n 2) 21–23, 25–33; European Commission, 'Common European Data Spaces' (Staff Working Document), SWD(2022) 45 final.
[70] See Commission, 'A European strategy for data' (n 2) 26–34.
[71] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM(2022) 197 final, arts 2(1)(b), (2)(c), (e), 3, 4, 34.
[72] Data Act, art 2(12), recital 18.
[73] See explicitly Data Act, recital 18. Cf Sections 5.1, 5.2.
[74] Data Act, recital 14 provides examples of these communication services.

the Internet of Things (IoT).[75] The definition excludes products whose primary function is the storing, processing or transmission of data on behalf of any other party than the user, such as servers or cloud infrastructure that are operated by their owners entirely on behalf of others.[76]

Article 2(6) Data Act defines 'related service' as a digital service that is connected to the product in such a way that its absence would prevent the product from performing one or more of its functions. It includes both services that are connected with the product at the time of purchase and services that have been connected to the product at a later time. Pursuant to recital 17, whether a service is related should be assessed in light of circumstances such as the content of the contract, what is normal for products of the same type, reasonable expectations of the user, and public statements by entities such as the seller or manufacturer. It makes no difference whether the services are provided by the provider of the product or by a third party. If there is doubt about whether the service is sufficiently connected to the product, the service should be considered 'related'. In this respect, the applicability of the Data Act to related services aligns with the applicability of the 'New Consumer Sales Directive' to the 'digital elements' of sold goods.[77]

The exact scope of the rights of access of the user has been subject to considerable debate during the legislative procedure of the Data Act. This debate was mainly focussed on the definition of 'product'. The Data Act proposal excluded all products whose primary function is the storing and processing of data, whether or not this was done on behalf of third parties.[78] Furthermore, recital 15 of the Data Act proposal excluded products that are primarily designed to display, play, record or transmit content such as personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners.[79] According to the recital, these products require human input to produce various forms of content. However, the Data Act does not clarify why this should lead to their exclusion.[80] Moreover, such products may also generate data without human input. For example, a smartphone could generate both photos (human input) and location data (no human input).

---

[75] Data Act, recital 14; Impact Assessment (n 6) 1.

[76] Data Act, recital 16.

[77] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28, art 2(5)(b), 3(3), recital 15.

[78] Data Act proposal (n 5), art 2(2). Cf Amendments (n 5), art 2(2).

[79] Cf Council of the European Union, '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) – Second Presidency compromise text (Chapters I–V)' (2022) 13342/22, art 2(2); Mandate (n 5), art 2(2). Although the presidency of the Council first proposed to add this exclusion to the definition of 'product', the Council ultimately decided to remove the exclusion from Article 2(2) altogether.

[80] Cf Mandate (n 5), recital 15; EDPB and EDPS, *EDPB–EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)* (2022) 14.

In the end, the legislators decided against strong restrictions of the covered products and services. Instead, the access of the user is limited to certain types of data. A user only has a right of access to 'product data' and 'related services data' or a subset thereof, the 'readily available data'.[81] It also has the right to access the 'metadata' that is necessary to interpret and use the data.[82] This includes data such as timestamps and other basic context.[83] In short, the rights of the user only apply to data that are generated through the use of the product or related service. Furthermore, they only apply to data that can reasonably be shared.[84] For this reason, 'product data' only refers to data that the manufacturer designed to be retrievable. Next, related service data only covers data that are recorded. Finally, the definition of 'readily available data' is limited to (product or related service) data that can be obtained without disproportionate effort.

5.4.2 The Content of the Rights

Chapter II Data Act creates several rights for the user. First, they are entitled to information. Pursuant to Article 3(2) Data Act, the contractual counterparty that sells, rents or leases the connected product should provide information about the characteristics, generation and storage of the generated product data and access by the user to this data. This information should be provided before the conclusion of the contract and in a clear and comprehensible format.

Article 3(3) Data Act creates a similar but more extensive right to information in connection to related services. Notably, it covers both product and related service data. Furthermore, the user should also receive information about the use of these data by, and the identity of, the data holder.[85] Again, this information must be provided before the conclusion of a contract, implying that the obligation rests with the contractual counterparty *of the service*. However, Article 3(3) Data Act is not explicit about this issue.[86] Instead, recital 24 states that the information should be provided by the prospective data holder, independently of whether it is the contractual counterparty *in relation to the product*. It does not address the possibility that the data holder is not the contractual counterparty *of the service*. In those situations, the Data Act thus does not provide a clear rule.

Next, the user has a right of access to the product and related service data. Pursuant to Article 3(1) Data Act, connected products and related services must be designed, manufactured and provided in such a matter that the product data and related services data are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and

[81] Data Act, art 2(15)–(17), recital 15.
[82] Data Act, arts 2(2), 3(1), 4(1), 5(1).
[83] Data Act, recital 15.
[84] See also Data Act, recital 20.
[85] Data Act, art 3(3)(c), (d).
[86] Cf Data Act proposal (n 5), art 3(2) (not explicit); Amendments (n 5), art 3(2b) (the provider of the service); Mandate (n 5), art 3(2) (the data holder).

appropriate, directly accessible to the user. The access can be granted, for example, with a user account or a mobile application provided with the product or service.[87]

This obligation is a notable addition to existing rights of access. It is imposed on the designers, manufacturers and providers of the connected products and related services. According the Data Act, these actors are often able to control the access to data, even when they have no legal right to the data themselves. Article 3(1) Data Act is designed to make sure that users can also obtain the data and to facilitate the development of more efficient and convenient services.[88]

In contrast, other obligations are primarily imposed on entities that hold or otherwise process the data, such as the controller of personal data or the public sector bodies and public undertakings that hold the documents.[89] The new obligation of the designers, manufacturers and providers is part of a broader development. European law increasingly imposes data-related requirements on products with digital elements. For example, the Delegated Regulation to the Radio Equipment Directive requires manufacturers, importers and distributors to ensure that internet-connected radio equipment incorporates safeguards to ensure the protection of personal data and privacy.[90] Next, the proposed ePrivacy Regulation requires that software permitting electronic communications offers the option to prevent third parties from storing or processing information on the terminal equipment of an end-user.[91] Finally, the cybersecurity requirements on products with digital elements imposed by the proposed Cyber Resilience Act are also intended to strengthen the protection of personal data.[92]

The Data Act also imposes a more 'traditional' obligation on the entity that holds the data: the 'data holder'. Article 4(1) stipulates that a data holder shall make readily available data accessible to the user if the user cannot directly access the data from the connected product or related service. The user also has a right to data portability under Article 5(1) Data Act. He can choose to have the data made available to a third

[87] Data Act, recital 21.
[88] Data Act, recital 20.
[89] GDPR, arts 15, 20; Open Data Directive, art 1(1).
[90] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L153/62, arts 3(3)(e), 10(1), 12(2), 13(2); Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3)(d), (e) and (f) of that Directive [2022] OJ L7/6, art 1(2)(a).
[91] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final, art 10(1).
[92] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020' COM(2022) 454 final, art 6(2)(c), recitals 17, 25.

party.[93] These rights are designed to foster the emergence of liquid, fair and efficient markets for data. According to the Data Act, the current lack of predictability of economic returns prevents businesses from making the necessary investments to share data.[94]

The requirements under Articles 4(1) and 5(1) are largely the same as under the right of access of Article 3(1) Data Act. Again, the data should accessible easily, securely, free of charge and in a comprehensive, structured, commonly used and machine-readable format. Furthermore, the data should be accessible continuously and in real-time where relevant and technically feasible.[95] Otherwise, the data should be provided without undue delay. Finally, the data should be of the same quality as is available to the data holder.

The rights of access and data portability of Articles 4(1) and 5(1) Data Act can be enforced against the data holder. This concept is defined in Article 2(13) Data Act. First, it refers to a person with an obligation to make data available under European law. In connection to the rights of access of the user, this leads to a circular reasoning: the obligation rests on the data holder, and the data holder is the person with the obligation.

More helpfully, the person who has a right to use data is also considered a data holder. The Data Act is not particularly clear about the exact origin of these rights. However, the recitals provide useful guidance. Most importantly, the Data Act does not grant the designer, manufacturer or provider a right to use the data that is generated by a connected product or related service. A separate ground is needed.

If the product or related service data contains personal data, the data can only be processed if there is a valid basis under Article 6(1) GDPR.[96] In this situation, the data holder is thus a controller or a processor within the meaning of the GDPR.[97]

If the prospective data holder, including the manufacturer, wishes to use non-personal data, it should do so on the basis of a contractual agreement with the user. According to recital 25, this should be the contract for the provision of the related service. This contract can be concluded in combination with the sale, rent or lease of the connected product itself. The provider of the related service will therefore typically be the data holder, even if it is also the manufacturer. This also explains why the information obligation in connection to related services is more extensive than for connected products, as discussed above. Furthermore, we see that the difference

[93] This right cannot be used to share data with a 'gatekeeper' under the Digital Markets Act. Data Act, arts 5(3), 6(2)(d), recital 40.
[94] Data Act, recital 26.
[95] Cf Data Act, art 3(1) ('directly accessible').
[96] Data Act, recitals 7, 34. See also Sections 3, 5.4.3.
[97] See also Data Act, recitals 22, 29, 34; Section 5.4.3.

between connected products and related services (Section 5.4.1) is crucial for the concept of the data holder.

The rights of the user in the Data Act complement the rights of information, access and data portability of the data subject under the GDPR.[98] They are more extensive in several ways.[99] They are not limited to personal data, can also benefit a user who is not the data subject and can be exercised against others than the controller.[100] Moreover, the Data Act requires, to the extent possible, direct (Article 3) or continuous and real-time (Articles 4 and 5) access. Under the GDPR, the controller has one or even three months to comply with a request.[101] Finally, the Data Act places additional requirements on the quality of the data. Both the GDPR and the Data Act require that the data are provided in a structured, commonly used and machine-readable format. The Data Act also stipulates that the data should be of the same quality as is available to the data holder.

The rights in the Data Act also have additional restrictions. First, they only apply to product and service data, or readily available data whereas the GDPR applies to all processed personal data.[102] Second, the rights in the Data Act do not apply to products and services of micro and small enterprises within the meaning of Recommendation 2003/361/EC. The GDPR does not contain such a 'size based' exception, other than the exclusion of household activities pursuant to Article 2(2)(c). Table 1 provides an overview of the differences between the Data Act and the GDPR.

Table 1: Comparison between the rights of access and data portability in the Data Act and GDPR

	Data Act	**GDPR**
Right of:	User	Data subject
Obligation for:	Data holder and manufacturer, designer or provider	Controller
Exception:	Micro and small enterprises	Household activities
What data:	Product and related service data, readily available data	Personal data
Quality:	Structured, commonly used and machine-readable format. The same quality as available to the data holder	Structured, commonly used and machine-readable format
Speed:	Directly, continuous and real-time if possible	One or three months

[98] Data Act, recitals 7, 24, 31, 34–35
[99] For an overview of the requirements in the GDPR, see also Wolters (n 20) 7–8, 10–11.
[100] See also Data Act, recital 35. See also n 102.
[101] GDPR, art 12(3); Wolters (n 20) 14.
[102] The right to data portability is limited to personal data that have been provided by the data subject. See also Article 29 Data Protection Working Party, *Guidelines on the right to data portability* (16/EN WP 242 rev.01, 2017); Wolters (n 20) 10.

5.4.3 Safeguards for the Protection of Personal Data

The product and related service data may include personal data.[103] However, the user is not always the data subject in relation to this data. A product can also be used by others, such as an employee of the user, or otherwise generate personal data relating to other people.[104] The Data Act contains safeguards for this situation. For example, Article 5(13) states that the new right to data portability may not adversely affect data protection rights of others.[105]

Most importantly, Articles 4(12) and 5(7) Data Act provide that the data holder shall only make the personal data of others available if there is a valid basis under Article 6(1) GDPR. The Data Act does not provide this basis.[106] The provisions are not clear about whether *the user or third party* that receives the data should have a legal basis for processing the requested personal data, or whether the *data holder* should have a legal basis for sharing the data. The formulation of the provisions, focussing on the act of sharing the data, point into the direction of the data holder. However, recital 34 shows that the provisions are meant to refer to the legal basis of the user or third party. A data holder may only share the personal data of others if the user or third party has a legal ground for the processing of these data.

The Data Act thus contains clear safeguards for the protection of personal data. However, these safeguards will apply and complicate data-sharing in many situations. Because of the broad definition of 'personal data' (Section 3), the generated data will often be personal data and frequently be related to other data subjects. Furthermore, these safeguards may not be practically feasible. They force the data holder to investigate whether personal data have been generated, to whom these data relate, to identify (and perhaps authenticate)[107] the user and to assess whether the user or third party has a valid basis to access someone else's personal data. All of these actions require additional processing of the personal data and thus adversely affect the right to data protection. Furthermore, the Data Act only provides limited guidance in this respect. For example, is the data holder supposed to check whether the data subjects have given their consent for the processing to the user? The data holder may not always be able to effectively perform these investigations, for example because it simply doesn't know the identity of the data subjects.

Most importantly, it is questionable whether these safeguards are necessary. The user or third party that receives the personal data will be bound by the GDPR. It will therefore be responsible to ensure the protection of personal data. Furthermore, the safeguards do not exist if the user can directly access the data through the product pursuant to Article 3(1) Data Act. The inclusion of the discussed safeguards is

---

[103] Cf Data Act, arts 4(12), 5(7), recitals 7, 34–35; EDPB and EDPS (n 80) 8.
[104] EDPB and EDPS (n 80) 10.
[105] About the issue of *silent party data* in the context of the GDPR and the PSD2, see also Wolters (n 20) 11; Wolters and Jacobs (n 15) 32–33.
[106] Data Act, recital 7.
[107] Cf Data Act, arts 4(5), 5(4), recitals 21, 29.

therefore not inevitable. It is the result of a trade-off between data protection and the free movement of data. On this issue, the Data Act prioritises data protection at the expense of the free movement of data. The safeguards limit the added value of the new rights, especially because they will almost always apply due to the broad definition of personal data.

5.5 The Access of Public Sector Bodies

Article 14 Data Act creates a right of access for public sector bodies, including Union institutions. It obligates a data holder to share data in case of an 'exceptional need'. The obligation only applies to data holders that are legal persons. Public sector bodies are excluded from the obligation.[108]

'Exceptional need' is broadly defined. Pursuant to Article 15(1)(a) Data Act, it exists if the requested data are necessary to respond to a public emergency and the public sector body is unable to obtain the data by alternative means in a timely and effective manner under equivalent conditions. 'Public emergency' is defined in Article 2(29). It means an exceptional situation that is limited in time such as public health emergencies, natural disasters and human-induced major disasters including major cybersecurity incidents. A public emergency must carry a risk of serious and lasting repercussions on the living conditions, economic stability, financial stability or the substantial and immediate degradation of economic assets. It must be officially declared as such according to the relevant procedures under European or national law. Pursuant to Article 15(1)(b)(i) Data Act, an exceptional need also exists if the data are necessary for any other specific task of public interest that has been explicitly provided by law. In this case, additional restrictions apply.[109]

If the request meets the conditions of Article 17 Data Act, the data holder is obligated to make the data available without delay pursuant to Article 18(1). This must be done free of charge if necessary to respond to a public emergency or for a compensation that covers the costs plus a reasonable margin.[110]

The Data Act contains several safeguards to ensure that the access of public sector bodies does not unduly affect the protection of personal data. Access to personal data should be proportional, limited to what is necessary and accompanied by data protection safeguards.[111] The personal data should be anonymised if possible. Otherwise, they should be aggregated or pseudonymised.[112]

Furthermore, personal data may only be requested if they are necessary to respond to a public emergency. They are excluded if the exceptional need relates to another

[108] See also Data Act, recital 63.
[109] See also Data Act, art 15(2) and the restriction to non-personal data discussed below.
[110] Data Act, art 20(1), (2). Cf the exceptions in Data Act, art 20(1), (3), (4).
[111] See in particular Data Act, arts 17(1)(c), (g), (2)(c), (e), (i), 19(1)(b), recital 72.
[112] Data Act, arts 17(1)(g), (2)(e), 18(4).

task in the public interest.[113] This restriction was added during the legislative process. The European Parliament even proposed to restrict the access to non-personal data in all situations.[114] In this light, the limitation of the access to personal data to public emergencies represents a compromise between data protection and the free movement of data.

At the same time, the access in case of public emergencies remains significantly more substantial than the other new obligations to share data discussed in Sections 5.2 and 5.4. First, this is due to the broad wording of 'public emergency'. Although this concept has also been restricted compared to the Data Act proposal,[115] it is still not limited to 'extreme' events such as terrorist attacks or nuclear disasters. Instead, it also covers situations which negatively affect the economic or financial stability or economic assets.[116] Furthermore, the safeguards are less restrictive than the safeguards in relation to the access of the user. The safeguards are designed to make sure that the access of public sector bodies does not affect the right to data protection more than necessary. As long as the processing of personal data is truly necessary to respond to the broadly defined public emergencies, a right of access to personal data exists. In relation to this right, the Data Act does opt for a clear strengthening of the free movement of data at the expense of the fundamental right to data protection.

6. Conclusion

The relationship between data and European law is characterised by two objectives that need to be balanced: data protection; and the free movement of data (Section 2). However, the strict interpretation of the GDPR has made sharing data difficult. The grounds for the lawfulness of a processing have been interpreted restrictively whereas the concept of personal data, and thus the scope of the GDPR, is interpreted broadly (Section 3).

The European strategy for data (Section 4) and the Data Act (Section 5) therefore focus on strengthening the free movement of data. However, most of the new rules do not seem to shift the balance significantly. Like the DGA (Section 4), the Data Act contains frameworks that apply *when* data are shared (Section 5.1). However, these frameworks do not ensure that data *will actually be shared*. The strict rules of the GDPR are not affected.

In this context, the Data Act represents a cautious approach. This is a fortunate choice. The general frameworks avoid stimulating the free movement of data through broad and blunt rules that can have large and unforeseen consequences and negatively impact data protection. At the same time, the frameworks do little to

[113] Data Act, art 15(1)(b).
[114] Amendments (n 5), art 14(1).
[115] The proposal did not contain the requirements that the situation was limited in time and officially declared an economic emergency. Cf Data Act proposal (n 5), art 2(10); Amendments (n 5), art 2(10); Mandate (n 5), art 2(10).
[116] See also EDPB and EDPS (n 80) 20–21.

achieve the objectives of the Data Act by themselves. Data protection is not adversely affected, but the strengthening of the free movement of data is only minimal. The general frameworks of the Data Act thus only provide a foundation that stimulates data-sharing on fair terms. They will only result in a strengthening of the free movement of data through other rights and obligations that build on this foundation.

Other parts of the Data Act do impose such rights and obligations. First, Article 23 Data Act obligates data processing service providers to ensure that customers can 'transfer' their data to other providers (Section 5.2). This provision also reflects a cautious approach. It creates a specific right that builds on existing codes of conduct and does not lead to substantial data protection risks. It thus strengthens the free movement of data without adversely affecting data protection. At the same time, the specific nature of this right means that its influence is limited. It will not fundamentally alter the balance between data protection and the free movement of data.

The general frameworks and the rules in relation to data processing services illustrate that the free movement of data and data protection are not always at odds. A cautious approach and specific rules can lead to a limited strengthening of the free movement of data without adversely affecting data protection. However, the new rights of access for IoT users and public sector bodies show that it is not always possible to have the best of both worlds. These rights also apply to personal data. Both rights are accompanied by safeguards for the protection of personal data. However, there is a clear difference in the way that they navigate the tension between free movement of data and data protection.

In relation to the access of the user, the Data Act prioritises data protection at the expense of the free movement of data (Section 5.4.3). Strict safeguards are imposed to make sure that this access does not adversely affect the right to data protection. A data holder can only share personal data if the user is also the data subject or if the user has valid legal basis to access this data. However, these safeguards may not be practically feasible. They limit the added value of the rights and may even have their own negative impact on data protection. Furthermore, the safeguards do not exist if the user can directly access the data through the product pursuant to Article 3(1) Data Act. The attempt to reconcile the free movement of data and data protection has thus led to a compromise in which neither interest is effectively promoted.

In contrast, the access of public sector bodies does lead to a meaningful strengthening of the free movement of data at the expense of the fundamental right to data protection (Section 5.5). This access also illustrates that it is not always possible to fully combine the free movement of data and data protection. In some situations, access to personal data is needed to effectively respond to a public emergency. In those situations, a choice between the free movement of data and data protection is necessary. Here, the Data Act prioritises the ability to effectively respond and thus the free movement of data. Although the Data Act contains various safeguards, a public sector body still has a right to access personal data as long as this is truly

necessary to respond to a (broadly defined) public emergency. At the same time, the final version of the Data Act is more cautious than the Data Act proposal. It restricts the access to personal data to public emergencies, whereas the proposal also allowed access to fulfil tasks in the public interest. The final version thus represents a compromise between the Commission, which proposed a broader access, and the European Parliament, which wished to restrict the access to non-personal data under all circumstances.

In this article, I answer the following research question: *How does the Data Act affect the balance between data protection and the free movement of data?* I have shown that the Data Act takes a cautious approach. It does not significantly affect the balance between data protection and the free movement of data *by itself*. Like the DGA, the Data Act creates extensive legal frameworks for data-sharing. However, the obligations and incentives to actually use these frameworks remain relatively limited. Without such obligations and incentives, data protection law will continue to impose a barrier.

This does not mean that the Data Act cannot play a meaningful role in the future. The Data Act is part of the broader European strategy for data. The extensive frameworks are not just meant for a few specific obligations to share data. They provide a foundation. It is up to other instruments such as the European data spaces to build on this foundation (Section 5.3). The impact of the Data Act on the balance between data protection and the free movement of data is therefore not set in stone. It depends on the success and further elaboration and implementation of the European strategy for data.