digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Andreas Sattler & Herbert Zech (eds.)

The Data Act: First Assessments

Band 19

Andreas Sattler & Herbert Zech (eds.)

The Data Act: First Assessments

digital | recht
Schriften zum Immaterialgüter-, IT-, Medien-, Daten- und Wettbewerbsrecht

Herausgegeben von Prof. Dr. Maximilian Becker, Prof. Dr. Katharina de la Durantaye, Prof. Dr. Franz Hofmann, Prof. Dr. Ruth Janal, Prof. Dr. Anne Lauber-Rönsberg, Prof. Dr. Benjamin Raue, Prof. Dr. Herbert Zech

Band 19

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.
Dieses Buch steht gleichzeitig als elektronische Version über die Webseite der Schriftenreihe: http://digitalrecht-z.uni-trier.de/ zur Verfügung.

ISBN: 9783759838865
URN: urn:nbn:de:hbz:385-2024072200
DOI: https://doi.org/10.25353/ubtr-04b0-0969-2b7a

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).
Anschrift der Herausgeber: Universitätsring 15, 54296 Trier.

Preface

In June 2023 the *Weizenbaum Institute*, the *Humboldt University of Berlin* and the *Center for Intellectual Property, Information and Technology Law* (CIPLITEC) held a workshop on the – then just politically agreed – Data Act (DA). The presentations by international experts shed light on the interface between the DA and important other fields of law that the DA will have a great impact on (for a summary of the workshop: *Rode*, The EU Data Act – Seamless Regulation or Urgent Need for Synchronisation?, GRUR 2023, 1255 – 1277).

The editors are very grateful that the workshop participants spontaneously agreed to contribute to this volume. Consequently, the results of the workshop can be made available to the many stakeholders addressed by the DA.

We thank *Jonathan Baumer* (Weizenbaum Institute) for his dedicated and immensely valuable support in editing this volume.

Karlsruhe/Berlin, June 2024

Andreas Sattler
Herbert Zech

Table of Contents

Part I

Economic Foundations

Chapter 1

Designing the Bundle of Rights on IoT Data: The EU Data Act

Martina Eckardt and Wolfgang Kerber*

A. Introduction

Internet of Things (IoT) devices are a new, fast-spreading innovation with many benefits but also new problems for which the current legal system does not yet have suitable solutions. The EU Data Act (DA) introduces new rights for users of IoT devices to access and use IoT data and share them with third parties to give users more control over their data (user empowerment) and to make more IoT data available for innovation and create more competition on secondary IoT-related markets for services (e.g., repair services).[1] The DA can be seen not only as introducing new rights on IoT data but also as a much more fundamental legislative act that attempts to design in a novel way the entire bundle of rights on data that are generated by the "Internet of Things": Who has what rights on what types of IoT data and can use, share, and monetize them? Therefore, the DA is also an important element in the necessary legal coevolution addressing

* Prof. Dr. Martina Eckardt, Professor of Public Economics and Public Finance, Andrássy University Budapest, Hungary, martina.eckardt@andrassyuni.hu; Prof. Dr. Wolfgang Kerber, Professor of Economics, University of Marburg, School of Business & Economics, Germany, kerber@wiwi.uni-marburg.de.

[1] Regulation (EU) 2023/2854 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 2023/2854, 22.12.2023, p. 1-71.

new problems arising from the "Internet of Things" as part of technological evolution.[2]

The objective of this article is to analyze how the DA changes the bundle of rights on IoT data and what its effects are on innovation, competition, and empowerment of users of IoT devices.[3] This article will focus primarily on non-personal IoT data because personal IoT data are already subject to the existing EU data protection law.[4] After a brief introduction into the economics of data and the bundle of rights approach from an economic perspective in section B, section C starts with an analysis of the governance of non-personal IoT data before the enactment of the DA, where up to now, the manufacturers of IoT devices have had exclusive de facto control over all IoT data. So far, this gives these data holders a property-like position on non-personal IoT data which results in not enough access, use, and sharing of IoT data with others. This has negative effects on innovation, competition, and choice of the users of IoT devices. Section Dexplains the objectives of the DA and its two key instruments (new user rights and a new contract about the use of non-personal data) for solving these problems. The main section E analyzes in two steps the change of the bundle of rights on IoT data (1) in the initial DA proposal of the European Commission, and (2) in the final version of the DA. This analysis uses three different concepts for the bundle of rights on IoT data: a data holder-centric concept, a user-centric concept, and the concept of co-generated data. It also discusses the implications of these changes for the effectiveness of the DA to achieve its objectives. Section F concludes and offers some further perspectives.

---

[2] For legal coevolution through technological change, see *Eckardt*, Technischer Wandel und Rechtsevolution, Die Einheit der Gesellschaftswissenschaften 118, Mohr Siebeck 2001; *Eckardt*, The evolution of the German tort law in the 19th century – An economic analysis of the evolution of law, 21 Homo Oeconomicus, 83-116, 2004; and with regard to the digital transformation, see *Kerber*, Digital revolution, institutional coevolution, and legal innovations, 34(6) European Business Law Review, 993-1016, 2023.

[3] This article is also based on *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113-143, 2024, which provides a more detailed economic and legal analysis.

[4] For the relationship between the DA and data protection law, see *Sattler*, Data Act and data protection law (Chapter 7 in this volume).

B. Theoretical framework: Bundle of rights on data and the relevance of market failures

From an economic perspective, the EU data policy is based upon the non-rivalrous character of data regarding its use, i.e. more access to and sharing of data can have many benefits, especially for innovation and competition. Depending on the type of data and the technological and economic conditions, the costs of generating data and the benefits of using it as much as possible can be very different. Therefore, a broad range of different governance solutions about who should have what kinds of rights to access, use, share, and monetize the data can be optimal from an economic perspective. This implies that we should be very cautious to apply too fast traditional well-established legal concepts like "property" on physical goods or IP rights to this new phenomenon of data which requires an own new legal approach. For data, it is necessary to use a very flexible concept that allows to design a wide range of different solutions for properly addressing the complexity of data governance problems.[5]

Such an approach is the bundles of rights approach, which has been used for a long time in the law but which can be derived also from the economic theory of property rights. Both the two extreme solutions of open data (public domain) and of exclusive IP-like rights of data can be analyzed and designed within the bundles of rights approach; this equally holds for many different intermediate solutions, like data access, sharing, portability rights and data trustee solutions.[6] However, for the question which bundle of rights solution is optimal, i.e. who should have which rights on a certain set of data, it is also relevant to take into

---

[5] For the economics and complexity of the governance of data, see *Martens*, Data access, consumer interests and social welfare, in: Drexl (ed.), Data access, consumer interests and public welfare, Nomos 2021, p. 69–102; *Martens*, A comparative economic perspective on EU data market regulations (Chapter 2 in this volume); *Kerber*, From (horizontal and sectoral) data access solutions towards data governance systems, in: Drexl (ed.), Data access consumer interests and public welfare, Nomos 2021, p. 441–476.

[6] For the link to the economic theory of property rights, see *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113 (117), 2024. For an application of the bundle of rights approach on data, see, more generally, *Kerber*, Specifying and assigning "bundles of rights" on data: An economic perspective, in: Hofmann/Raue/Zech (eds.), Eigentum in der digitalen Gesellschaft, Mohr Siebeck 2022, p. 151–176.

account how well markets work because rights can be reallocated through trading them. Therefore, it is necessary to analyze whether market failures exist (e.g., market power problems, information asymmetries, behavioral problems, transaction costs) and to what extent such problems are solved by legal rules and regulations. For our analysis of the bundle of rights on IoT data this implies that also the question of market failures on the market for IoT devices and on the markets for non-personal and personal data have to be considered.

C. The current bundle of rights on IoT data and its problems

The current bundle of rights on IoT data can be described as follows. The manufacturers can design technically the IoT devices in such a way that they get exclusive de facto control over all data that is generated by the users with these devices - usually by directly transmitting the data to a proprietary server and through their technical control over the IoT device. As a consequence, they can "capture" this fast-increasing amount of IoT data, which is a new valuable resource. As far as this data is personal data, EU data protection law provides the users as data subjects with a set of rights on their personal IoT data. In addition, the data holders usually need a contract with the users for the processing, use, and sharing of this personal data ("consent"; Art. 6(1)a GDPR). For non-personal IoT data, however, often no de-jure rights exist. Therefore, the manufacturers as holders of this data are free to use, share, and monetize it. Vice versa, the users as owners of the IoT devices as well as other firms who would also like to use this data are excluded from this data through the technological design of the IoT device. Therefore, so far, the data holders have de facto a property-like position with regard to non-personal IoT data. Thus, they can exclusively extract the value from the data as if they were the "owners" of this data. Through such a strategy of technological capture of the IoT data, the manufacturers can de facto "appropriate" the non-personal data.[7] From an economic perspective, the "bundle of rights" on non-personal IoT data is de facto assigned exclusively

[7] See *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113-143, 2024; *Kerber*, Governance of IoT data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120, 2023; and similar *Lundqvist*, Regulating Access and Transfer of Data, Cambridge University Press 2023, p. 6-56.

to the data holders through their own technological decisions, although they do not have any legal rights on this data.

This exclusive control of the manufacturer over the IoT data has led to a number of serious problems, which were also the main motivation for the Commission for initiating the DA project. It gives the manufacturers a powerful gatekeeper position vis-a-vis the users of the devices and many other firms who need access to this data to offer additional services on secondary markets and to innovate new products and services. This exclusive monopolistic position on these non-personal data can also lead to a systematic under-use of this non-rivalrous resource, e.g. through too high data prices and restrictive conditions for accessing and using the data. Therefore, from a competition and innovation policy perspective, this current form of the governance of IoT data is expected to have negative effects on innovation and competition due to a lack of access to and sharing of IoT data, especially on secondary markets in digital IoT ecosystems.[8] In addition, large concerns have been raised that the owners and users of the IoT devices do not get enough control over their IoT data, and that they would not get a fair share of the value from this data.

D. The approach of the Data Act: An overview

The DA has understood very well the above-described problems of the current governance of IoT data, especially the negative effects of exclusive de facto control over IoT data for innovation, competition on secondary markets, and the lack of control of users over the generated IoT data. This leads to the objectives of the DA: It wants to make more data available for the innovation of products and services and for protecting and enabling competition on secondary markets. It also intends to enhance the empowerment of users and to provide more fairness regarding the distribution of the value of this data. But the DA also wants

[8] For an overview on these problems, see *Kerber*, Governance of IoT data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120 (122), 2023; for the example of connected cars, see *Kerber*, Data governance in connected cars: The problem of access to in-vehicle data, 9 JIPITEC 310, 2018; and, most recently, *Wiebe/Helmschrot/Kreutz*, Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft, Studie im Auftrag der Bundesnetzagentur, February 2023.

to preserve the incentives of IoT manufacturers to invest in data-generating IoT devices.[9]

The DA, however, does not challenge the freedom of manufacturers to design their IoT devices in such a way that they get exclusive de facto control over the data. The DA accepts the technological capturing of this data by the manufacturers and their technological control over the IoT devices. Therefore, the main strategy of the DA is to limit the negative effects from the exclusive de facto control position of the manufacturers through a set of mandatory rules for the governance of IoT devices to solve these problems.

The DA wants to achieve its objectives by two key instruments and a technological precondition about the governance of IoT data:

(1) New rights for the users regarding access, use, and sharing of IoT data: Art. 4 and 5 DA introduce new rights of the users of the devices to access and use the IoT data (Art. 4) and to share them with third parties (Art. 5). The scope of the IoT data for these rights, however, is limited to raw data and "pre-processed" data, and does not encompass inferred and derived IoT data.[10] Users can freely decide with whom they want to share IoT data and for what purposes (e.g., for the provision of services or for innovation), but the data holders can require a (licensing) contract with the data recipients and claim "reasonable compensation" (with FRAND conditions).[11]

(2) New data use contract between data holders and users: In addition to the agreement about the processing, use, and sharing of personal IoT data (consent according to Art. 6(1) a GDPR), the DA introduces the requirement of a new contract about the use of non-personal IoT data by the data holder (Art. 4(13) DA). This implies that without such an agreement with the users, the data holders cannot anymore use, share, and monetize the non-personal IoT data that are under their exclusive de facto control.

An important precondition for these two key instruments is the obligation in Art. 3 DA that manufacturers have to design their IoT device technologically in

---

[9] See European Commission, Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23.2.2022, COM(2022) 68 final [Draft DA], Explanatory Memorandum, p. 2-3.

[10] See recital 15 DA.

[11] See Art. 8 and 9 DA.

such a way that this IoT data are easily accessible for the users and can be shared with third parties as data recipients.[12]

E. The change of the bundle of rights by the EU Data Act

I. Introduction

One of the main problems of the DA is that it is not based on a clear and consistent concept about the bundle of rights on IoT data, neither from a legal nor from an economic perspective. We show in this section that this is not only true for the initial proposal of the Commission. Overall, also the changes introduced during the legislative process have not led to a more coherent and effective approach. Therefore, it cannot be expected that the objectives of the DA will be achieved. From our analysis of the proposal and the final version of the DA as well as from the academic and legislative discussions, we identify three different concepts for the bundle of rights on non-personal data, which have been used in the reasoning about the DA, albeit often in a more implicit way. They can be briefly summarized as follows:[13]

(1) Data holder-centric concept: Largely based upon the status-quo situation, in this concept the manufacturers (and data holders) are seen as the "owners" of this data. Due to an alleged incentive problem regarding investing in data-generating IoT devices, according to this concept the data holders also should have a far-reaching IP-like "bundle of rights" on this non-personal data with the possibility to extract most of the value from this data.

(2) User-centric concept: An alternative concept would assign the bundle of rights on this non-personal data to the users of these IoT devices. These are usually also the owners of these physical devices that they have bought from the manufacturers. This concept has some parallels with the current legal situation regarding personal IoT data in the EU.

---

[12] Art. 3 DA also encompasses transparency requirements about the generated data, e.g. what types of data, whether it is generated continuously and in real-time, and how to access the data etc.

[13] For an in-depth analysis of each of these concepts, see *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113-143, 2024.

(3) Concept of co-generated data: This concept is based upon the wide-spread notion that in the data economy often more than one actor contributes to the generation of data. Therefore, all co-generators should have rights on this data and participate in the value of this data. With regard to IoT data, the DA views both the manufacturers and the users as contributors to the generation of non-personal IoT data.[14]

In the following subsections, we analyze how and to what extent the DA proposal and the final version of the DA use elements from these three different concepts, and what contradictions and problems arise through the lack of applying a clear concept. In addition, we examine whether the two key instruments introduced by the DA – as presented in section D - can be expected to provide an effective legal solution for achieving the objectives of the DA. This also requires to explore whether the DA correctly identifies and solves existing market failures in B2C and B2B contexts because - as explained in section B - the optimal design of the bundle of rights depends as well on the extent that markets are not suffering from significant market failures.

II. Analysis I: Bundle of rights in the DA proposal of the European Commission

The initial DA proposal of the Commission[15] is still much dominated by the currently strong position of manufacturers with their exclusive de facto control over IoT data. It is therefore closely aligned to the above described data holder-centric concept. Most of the rules in the DA proposal about IoT data fit very well to an interpretation that the data holders should have an IP-like position on non-personal data. The DA strongly emphasizes the incentives to invest in data-generating IoT devices, suggesting the need for data holders to monetize the IoT data, which is close to a typical IP justification. Although the DA explicitly states that it does not confer any new rights on non-personal data to the data holders, it clearly acknowledges and protects the exclusive de facto control position over all IoT data. This is done e.g., by allowing to make data accessible only "in-situ" (e.g., on servers controlled by the data holders) and by giving the data holders the right to require technical protection measures in the case that these IoT data

[14] See recital 6 DA.

[15] See European Commission, Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23.2.2022, COM(2022) 68 final.

are shared via the data sharing right of the users with third parties.[16] This interpretation that the data are seen as "owned" in an IP-like way by the data holders is also supported by the requirement of a negotiated licensing contract between the data holder and a data recipient with whom the users share the data for a certain purpose.[17] The DA proposal also defines the scope of the data for the data rights very narrowly (only raw data), whereas all other IoT data, and, in particular, derived and inferred data remain under the exclusive de facto control of the data holders (preserving their de facto ownership position on this data).[18]

In the DA proposal of the Commission, however, also important reasoning and rules can be found that do not fit to and even directly contradict such a data holder-centric approach:

(1) The view of the DA that IoT data are co-generated by manufacturers and users seem to contradict the concept of an exclusive "ownership" by data holders. This holds also for the introduction of new user access and sharing rights. However, it is not unusual in IP law that the exclusivity of IP rights has limitations with also other actors having rights for use (e.g., "fair use" in copyright law). Nevertheless, the provisions that allow the users to decide nearly entirely free on how to use this IoT data, with whom to share it and for what purposes, do not fit to a data holder-centric approach.

(2) Particularly important is that the data holders lose their currently existing "de facto ownership" of non-personal data through the second key instrument because for using, sharing, and monetizing the IoT data they now need a contract with the users of the IoT device (Art. 4(13) DA).[19] This can be interpreted as a fundamental change in the assignment of the bundle of rights on non-personal IoT data from the data holders with their exclusive

---

[16] See, e.g., Art. 4(11), 5(5) and recitals 8 and 22 ("in situ access", i.e. data holder need not provide a copy of the data to the user or third-party). If the data are only made accessible and useable "in-situ", then the user can not directly share this data with other firms (and "circumvent" the data sharing mechanism of Art. 5 DA). These rules apply independently from the question whether the data are also trade secrets.

[17] However, the data holder is not free in setting a "licensing fee" but can only claim a "reasonable compensation" which, nevertheless, can also entail a profit margin.

[18] Therefore, the introduction of these user rights do not change the bundle of rights for those IoT data which are outside of the scope of these user rights. The exclusion of all inferred and derived IoT data can significantly reduce the usability of the data that can be accessed, used, and shared with these user rights.

[19] This was Art. 4(6) in the DA proposal of the Commission.

de facto control to the users of the IoT devices:[20] Whereas now the data holders need the consent of the users for using the data, the users have the right to access, use and share this non-personal data without needing the consent of the data holders.[21] This change in the bundle of rights through this new contract was partly heavily criticized in the academic discussion, including demands for the deletion of this new contract.[22]

A deeper analysis of the two new key instruments in the DA proposal, however, shows that both of them can be expected to be very weak and largely ineffective.

(1) The new user rights for access and sharing of IoT data with other firms suffer from too many restrictions, hurdles, and high transaction costs: Bilateral negotiations between data holders and data recipients about reasonable compensation (with FRAND conditions) as well as technical protection measures, disputes about trade secret protection, and open questions about compliance with data protection law are only some of the problems. In addition, the scope of the shared data is often not sufficient for providing additional services (e.g., repair services) and for enabling innovation. Therefore, the data sharing mechanism via the users often will not be effective, and therefore will not lead to much additional sharing of IoT data, more innovation, and competition on secondary markets.[23]

---

[20] See *Hennemann/Steinrötter*, Data Act – Fundament des neuen Datenwirtschaftsrechts? Neue Juristische Wochenschrift 2022, 1481 (1483); *Specht-Riemenschneider*, Der Entwurf des Data Act, MMR, Zeitschrift für IT-Recht und Recht der Digitalisierung 2022, 809–826; *Wiebe*, Der Data Act–Innovation oder Illusion? GRUR 2023, 1569 (1570).

[21] The DA does confer new rights on this non-personal IoT data only to the users but not to the data holders (see also recital 5 DA).

[22] See *Drexl* et al., 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), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, https://doi.org/10.2139/ssrn.4136484, para. 44-54; *Leistner/Antoine*, 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 Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs, 2022, https://doi.org/10.2139/ssrn.4125503, p. 92-95. One main argument was that the manufacturers might be more motivated and better capable to use and share the data.

[23] In much more detail wee *Kerber*, Governance of IoT data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120 (125-128), 2023; *Podszun/Offergeld*, The EU Data Act and the access to secondary markets. Study for the Ludwig-Fröhler-Institut für

(2) At least in B2C contexts, it also cannot be expected that the new data use contract regarding non-personal data will give the consumers much more meaningful control over their data and will lead to a fairer share of the value of their IoT data: Consumers will suffer from the same information and behavioral problems (including behavioral manipulation) as in the case of personal data where "notice and consent" solutions do not work sufficiently. In addition, IoT device manufacturers can bundle the contract about the sale of the IoT device with a "buy-out" contract about their use, sharing, and monetizing of the non-personal IoT data. This "contracting away" of the bundle of rights on non-personal data would lead back to the exclusive control of the data holders over the IoT data (but now based upon a contract instead of technical de facto control).[24]

From an economic perspective the DA proposal of the Commission suffered from serious mistakes regarding its assumptions about market failures. (1) It mistakenly claimed that a serious general incentive problem exists for investing in data-generating IoT devices. But since manufacturers can cover their investment costs through the price of the IoT device, such a general incentive problem does not exist.[25] (2) The DA does not sufficiently take into account the information and behavioral market failures of consumers. Therefore, it should not rely on pure freedom of contract for the data use contract between data holders

---

Handwerkswissenschaften, 2022, https://doi.org/10.2139/ssrn.4256882. Particularly important is also the lack of solutions for technical interoperability which is often necessary for certain complementary services, as e.g. repair and maintenance services.

[24] See *Specht-Riemenschneider*, Der Entwurf des Data Act, MMR, Zeitschrift für IT-Recht und Recht der Digitalisierung 2022, 809 (820); *Kerber*, Governance of IoT data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120 (132), 2023; *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113-143, 2024; for an analysis of this problem in B2B contexts, see section E.III below.

[25] See *Drexl* et al., 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), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, https://doi.org/10.2139/ssrn.4136484, para. 72; *Specht-Riemenschneider*, Der Entwurf des Data Act, MMR, Zeitschrift für IT-Recht und Recht der Digitalisierung 2022, 809 (823); *Martens*, Pro- and anti- competitive provisions in the proposed European Union Data Act, Working Paper 01/2023, Bruegel 2023; and *Kerber*, Governance of IoT data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120 (128-130), 2023.

and consumers without providing additional regulatory measures for protecting the interests of consumers.[26] (3) However, the DA proposal has correctly understood that exclusive control over IoT data is not the best solution due to the non-rivalrous character of data. But due to its mistaken assumption of an unsolved incentive problem for manufacturers, it wrongly favored more the interests of the manufacturers instead of focusing more on the many advantages of more access and sharing of IoT data for the users and for innovation and competition. This wrong balancing of interests might also be the main reason why so many restrictions and hurdles, which mostly protect the data holders, have been implemented in the data sharing mechanism, thus rendering it weak and ineffective.

Although the proposal of the Commission attempted to address the right problems and introduced two new and interesting key instruments for achieving its objectives, a broader assessment from an economic perspective comes to the conclusion that it cannot be expected to achieve its objectives, especially with regard to more innovation, competition, and user empowerment.[27] Due to the mentioned contradictions between a strong alignment with a data holder-centric approach and important elements from a user-centric approach, as well as by including elements from the concept of co-generated data, the DA proposal also did not succeed in developing a coherent design for the bundle of rights on non-personal IoT data.

III. Analysis II: Further changes in the final version of the Data Act

In the further legislative negotiations between the European Parliament, the Council and the Commission (so-called Trilogue), a number of interesting additional changes have been made in the DA, also with regard to the bundle of rights on non-personal data. We will see, however, that regarding both the coherence and the effectiveness of the DA it is unclear to what extent these changes have improved it. In the following, only the most relevant changes are analyzed.

---

[26] The new transparency requirements in Art. 3 DA can help only to some extent.

[27] See, e.g., *Kerber*, Governance of IoT data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120 (133), 2023; *Lundqvist*, Regulating Access and Transfer of Data, Cambridge University Press 2023, 102-108; and *Wiebe*, Der Data Act–Innovation oder Illusion? GRUR 2023, 1569 (1578).

Particularly important is that the controversially discussed data use contract between data holders and users has been confirmed and strengthened in the final version of the DA. The provision that the data holders need a contract with the users for using the non-personal IoT data (Art. 4(13) DA) has been complemented with an additional Art. 4(14) DA that includes additional restrictions for the data holders regarding the sharing of data generated by an IoT device (product data). Moreover, the new recital 26 states that only the users are allowed to monetize this product data. The main argument is that such an exclusive assignment of the right to monetize the non-personal IoT product data gives users larger incentives to share the data. This would enable that the data sharing right (Art. 5 DA) can lead to the emergence of "liquid, fair and efficient" data markets which, in turn, would have positive effects on innovation and competition.[28] Whereas the DA proposal of the Commission was always unclear whether it wanted to open a path to such data markets, the final version of the DA now clearly states that it wants such data markets via these user rights and that only the users should have the right to monetize the data. In this context, the DA sees now also a clear role for data intermediaries (as defined and regulated in the Data Governance Act), who can be used by the users, also for monetizing their data. However, the users can also monetize their IoT data via the data holders or other firms. All in all, these new provisions and recitals strongly support that in the final DA the bundle of rights on IoT data has been assigned primarily to the users of IoT devices.

These modifications in the legislative process could be interpreted as a major change in the basic architecture and concept of the DA from a primarily data holder-centric approach in the proposal to a much more user-centric approach in the final DA. However, many other provisions in the DA proposal which are based upon the data holder-centric concept have not been changed, they have even been strengthened to some extent. Although it is now much clearer than in the proposal that it is the user who is licensing the IoT data to the data holders (or other firms), the data holders still can claim "reasonable compensation" from the firms with which the users are sharing their IoT data. This does not fit to a concept in which the users get exclusive rights to use, share, and monetize their non-personal IoT data. The same is true for many provisions in the DA that

[28] Recital 33 DA; important is that in the final version Art. 6(2)(c) DA now explicitly allows that data recipients can "resell" the data to other firms if users agree.

protect and strengthen unilaterally the de facto control position of the data holders vis-a-vis the users and data recipients.

The notion that this IoT data should have an IP-like protection has also been strengthened to some extent in the final version because during the Trilogue negotiations many concerns have been raised that a lot of this IoT data might be trade secrets of the manufacturers. This has led to strong demands for a stronger protection of trade secrets with respect to the data sharing obligations of the data holders. As a consequence, the data holder-centric concept with regard to IoT data has been strengthened in the final version through a number of changes (including exceptions to the data access and data sharing obligations of Art. 4 and 5 DA).[29]

Will these changes in the final version of the DA lead to a better achievement of its objectives by making the two key instruments more effective? In the following, we will distinguish between B2C and B2B contexts.

Data use contract (Art. 4(13) DA) in B2C contexts: Although the clearer assignment of the rights on non-personal data to the users strengthens conceptually the key role of the data use contract between data holders and users, this change of the bundle of rights might not help to give the users more effective control over their non-personal data and prevent buy-out contracts regarding this IoT data. The information and behavioral problems of consumers still exist,[30] and the manufacturers can still as easily contract away these rights by bundling this contract with the sale contract as in the initial DA proposal.[31] Even the explicit exclusive assignment of the right to monetize the non-personal IoT

---

[29] See, e.g., Art. 4(6)-(9) DA and recital 31. For the complex discussion about the relationship of trade secret law and DA, see *Wiebe*, The Data Act proposal. Access rights at the intersection with database rights and trade secret protection, GRUR 2023, 227–238; *Aplin*, The Data Act and trade secrets: an experiment in compulsory licensing (Chapter 6 in this volume); *Zech*, Data access rights as property rights (Chapter 4 in this volume).

[30] However, in the final version a new prohibition against behavioral manipulation of the user by the data holders was included (Art. 4(4) DA).

[31] An amendment of the EP to limit the bundling of these contracts failed in the final negotiations about the DA: "The data holder shall not make the use of the product or related service dependent on the user allowing it to process data not required for the functionality of the product or provision of the related service" (Art. 4(6) s.2 Draft European Parliament Legislative Resolution 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) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD)).

product data to the users in the final version of the DA does not change this. In B2C situations such a bundling strategy still implies that the consumers are only left with their non-waivable user rights which cannot be contracted away.[32] It is also unclear whether these market failure problems and bundling strategies of the manufacturers will not counteract the objective to enable the consumers to get a larger share of the value from their IoT data. It is one of the problems in the final DA that it still relies on a pure freedom of contract approach without the necessary measures for dealing with the market failure problems regarding consumers.

What are the effects of these changes in B2B contexts? It was unclear from the beginning whether here a general market failure exists at all and why the question of the allocation of rights to access, use, and share non-personal data cannot be left to free negotiations between manufacturers and business users on the market. While unequal bilateral bargaining power can also be a market failure problem in B2B situations, this will happen only in a limited group of cases.[33] Thus, it is not surprising that the application of the same rules in B2C and B2B situations about new user access and sharing rights and the data use contract in the proposal of the Commission was much criticized.[34]

Therefore, it has to be welcomed that the final version has tried to react to demands for a stronger differentiation between B2C and B2B situations through an important additional change in the design of the bundle of rights: In B2B situations, it now allows business users to "waive" their new user rights on non-personal data (Art. 4 and 5 DA) (for a "proportionate compensation").[35] This can have many positive effects because it leads back to the principle of freedom of contract and helps to avoid over-regulation in many B2B situations. However, it also raises the question why the mandatory introduction of new but waivable user rights will lead to more access, use, and sharing of IoT data, and therefore to more innovation, competition, and user empowerment. In B2B situations, the manufacturers can also bundle the sale of a smart machine with a

---

[32] This also shows the importance of the non-waivability of these user rights in B2C contexts.

[33] Even if this is the case, it is not always the manufacturers who are in the stronger position as assumed by the DA. Often business users can have superior bargaining power which leads to the problem that now the manufacturers have no access to the IoT data.

[34] See, e.g, *Metzger/Schweitzer*, Shaping markets: A critical evaluation of the Draft Data Act, Zeitschrift für Europäisches Privatrecht 2023, 42 (56-58).

[35] Recital 25 DA.

contract in which the business users waive their new user rights. In this case, there might not change much compared to the situation before the DA, i.e. the manufacturers have exclusive control over all generated IoT data but now on a contractual basis. With enough bargaining power, the manufacturer can contract away all rights that the DA grants to the business users, including the exclusive rights to monetize this data. If manufacturers do not have such unequal bargaining power vis-a-vis business users, then the latter can negotiate the efficient solutions for the access, use, or sharing of the IoT data also without the rules of the DA. Therefore, it is not clear why the DA should lead to the unlocking of more IoT data in B2B contexts and therefore to more innovation and competition.[36]

Will the changes in the final version of the DA lead to a larger effectiveness of the data sharing mechanism of Art. 5 DA than in the initial proposal of the Commission? The extension of the scope of the IoT data for the user rights by including not only raw data but also "pre-processed" data is at least a small improvement. It can make the shared data more usable for data recipients, but it is very unclear whether this really changes much for enabling complementary services and innovation. Most important is, however, that the restrictions, hurdles, and transaction costs of the data sharing mechanism have not been reduced in the final version of the DA. On the contrary, instead of simplifying the mechanism, additional requirements and hurdles have been introduced. Particular important are the new provisions that strengthen the possibilities for data holders to use claims about trade secret protection of (raw and pre-processed) IoT data for making it harder to share these data, and more expensive and unattractive for data recipients to use such data.[37] Important is also that the two provisions which directly limit the sharing of IoT data and protect the manufacturers of IoT devices against competition have been confirmed and strengthened in the final version of the DA. The DA prohibits that the users and the data recipients use the shared IoT data for developing a product which competes with the IoT devices that have generated this data. In addition, the users are also not allowed to share their IoT data with firms that are designated as gatekeepers in the Digital

---

[36] It is also not clear why the business users should have generally more incentives for sharing the data than the manufacturers. This depends much on the business models of manufacturers and users.

[37] Also other additional provisions were included that can further weaken the data sharing mechanism.

Markets Act.[38] However, the already described changes for enabling and supporting new markets for non-personal data and the possible active role of data intermediaries in that respect might be a very important positive step that could lead to more unlocking of IoT data and innovation, e.g. through the building of aggregated data sets. But it will be one of the important tasks to clarify how the complex rules of the DA can be applied in such a way that well-functioning data markets for non-personal data can emerge.

F. Conclusions and perspectives

The EU Data Act sets new rules for the governance of data generated by IoT devices. The GDPR already stipulates that consumers must consent to the use of their personal data by others. This holds also for personal data generated by IoT devices. However, so far there were no provisions in place regarding non-personal data. This allowed the manufacturers of IoT devices to technically capture the data through the design of their IoT devices. With the Data Act, the European Commission now wants to achieve that users of IoT devices have more control over their data and get a fair share of its value and that more data is made available to third parties for innovation and competition, in particular on secondary markets. To these ends, the DA introduces two novel provisions which for the first time assign access, use, and sharing rights to users of IoT devices. In addition, it requires manufacturers to get the consent of users via a contract for also using these data. In this paper, we analyzed how the DA will change the bundles of rights on non-personal IoT data and whether it can be expected that the DA achieves its objectives.

Our main findings can be summarized as follows.[39] The DA is not based upon a clear legal or economic concept and is therefore unclear and contradictory regarding its design of the bundle of rights on non-personal data. Although the final version of the DA has clarified some issues, it also has led to new open

---

[38] See, e.g. Art. 4(10) and Art. 5(3) DA. For a critical analysis see *Metzger/Schweitzer*, Shaping markets: A critical evaluation of the Draft Data Act, Zeitschrift für Europäisches Privatrecht 2023, 42 (59-61); and *Kerber*, Data Act and competition: An ambivalent relationship, Concurrences 2023, No.1, 30–36.

[39] For a broader analysis, see *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113 (136-139), 2024.

questions and contradictions, e.g. between the application of a data holder-centric and a user-centric approach. Although the latter has been conceptually strengthened by explicitly assigning the bundle of rights on the use, sharing, and monetizing of the IoT product data to the users, it is very unclear whether this will give the users more effective control over their IoT data. The DA does not protect the users against the potential strategy of the data holders to bundle the sales contract about the IoT device with a far-reaching buy-out contract about the use of non-personal data. The newly assigned rights on non-personal data to the users can therefore be contracted away, especially in B2C situations, i.e. the control over the non-personal data can again end up exclusively with the data holder. In B2B situations, this can be different depending on the bilateral distribution of negotiation power.

Another important finding is that in the final version of the DA the concept of co-generated data does play an even smaller role than in the initial proposal of the Commission. Instead of opening access to the data which are non-rivalrous in use, the DA seems to assign an exclusive bundle of rights over raw and pre-processed IoT data to the users of the IoT devices. In the academic discussion on the DA proposal, several authors suggested an application of the concept of co-generated data in which both the data holders and the users should have independent sets of rights to use, share, and monetize the non-personal data.[40] This would also have the advantage that if one actor does not want to share the data, then access and sharing of the data might still be possible via the other contributor to the generation of data. This could be very helpful regarding the objectives of the DA of enabling innovation and competition.[41] However, the final version of the DA with its emphasis on an exclusive assignment of the bundle of rights on data to the users and many options how the data holders can ensure their exclusive control over the non-personal IoT data (via contracts), is on a dangerous path and slippery slope to fall back to mistaken concepts of exclusivity as an optimal governance solution for data that are non-rivalrous in use.

---

[40] See *Metzger/Schweitzer*, Shaping markets: A critical evaluation of the Draft Data Act, Zeitschrift für Europäisches Privatrecht 2023, 42 (50-51); *Martens*, Pro- and anti- competitive provisions in the proposed European Union Data Act, Working Paper 01/2023, Bruegel 2023, p. 20, who suggested a "mutual exhaustion" of their rights on IoT data.

[41] See *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113 (132-135), 2024.

Overall, the DA can still not be expected to achieve sufficiently its objectives of (1) unlocking much more IoT data for innovation and competition, especially on secondary markets, (2) giving users, in particular, consumers, more meaningful control over their IoT data, and (3) improve significantly the fairness of the distribution of the value from the IoT data although explicitly allowing markets for the shared non-personal data might help to some extent. A big problem is that the basic contradictions, open questions, and unclear provisions can lead to great deal of legal uncertainty due to very different interpretations of the rules of the DA and the specific design of the bundle of rights on IoT data. This also includes the relationship to other laws, such as data protection and trade secret law, which also determine important parts of the bundle of rights on IoT data.[42]

Therefore, it is necessary to think about further improvements of the DA and additional policies. Regarding the DA itself, a streamlining of the data sharing mechanism of Art. 5 DA by reducing the many hurdles, restrictions, and transaction costs would be very important in order to improve significantly its effectiveness. For enabling more innovation, it is also important to ensure that emerging markets for non-personal data can work effectively in practice and are not impeded by the too complex rules of the DA. With regard to the objectives of more empowerment of consumers as users of IoT devices and a fairer sharing of the value of IoT data, it is necessary to introduce additional consumer protection measures which enable consumers to get more control over their data and participate more in the value of their consumer data. In that respect, it is an interesting question whether the DA, which covers both non-personal and personal IoT data, can also be used to better empower consumers regarding their personal data and can therefore complement the GDPR and thus help it in achieving its objectives.[43] However, also additional policies beyond the DA with

---

[42] A broader analysis would also include into the analysis of the bundles of rights on IoT data trade secret law, data protection law, and copyright law; see for copyright law *Raue,* "Without prejudice": The interface of the Data Act and copyright (Chapter 8 in this volume), and *Wiebe*, The database right and Art. 43 of the Data Act (Chapter 9 in this volume).

[43] The data sharing right of Art. 5 DA goes far beyond the data portability right of Art. 20 GDPR.

its user-initiated data sharing mechanism will be necessary:[44] This implies additional regulations for direct access rights of firms to IoT data, e.g., new sectoral regulations (like an updated type approval regulation for motor vehicles) and regulations for getting access to IoT data for training AI-based algorithms. New innovative data trustee solutions for certain sets of IoT data might also lead to additional positive effects for supporting the unlocking of IoT data and more innovation and competition.

---

[44] See *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the EU Data Act, 57 European Journal of Law & Economics 113 (135), 2024; *Eckardt*, Data commons and the EU Data Act in: Heine/Budzinski (eds.), Wettbewerb, Recht und Wirtschaftspolitik, Festschrift für Wolfgang Kerber, Nomos 2024, 241-257.

Chapter 2

A comparative economic perspective on EU data market regulations

Bertin Martens*

A. Introduction

In 2020, the European Commission published a new European Strategy for Data comprising a series of regulatory interventions in data markets[1]. This resulted in several horizontal or cross-sectoral data regulations, including the Data Governance Act[2], the Data Act[3] and sector-specific regulations, such as the European Health Data Space[4] and several sectoral data-pooling initiatives in agriculture, transport, energy, etc. Moreover, the Digital Markets Act[5], a competition policy tool that targets very large digital 'gatekeeper' platforms, also includes data-access obligations. While it is too early to assess their actual economic impact, this chapter compares and assesses the potential economic impact of

* Dr. Bertin Martens, Senior Research Fellow, Bruegel economic policy think-tank in Brussels, Belgium, and non-resident fellow, Tilburg Law and Economics Centre, Tilburg University, Netherlands.

[1] European Commission, Communication for the Commission to the European Parliament and the Council, A European strategy for data, 19.2.2020, COM(2020)66 final.

[2] Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act), OJ L 152, 3.6.2022, p. 1-44.

[3] Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), OJ L 2023/2854, 22.12.2023, p. 1-71.

[4] European Commission, Proposal for a regulation of the European Parliament and the Council on the European Health Data Space, 3.5.2022, COM(2022)197 final.

[5] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L 265, 12.10.2022, p. 1-66.

three of these EU data market regulations: the European Health Data Space (EHDS), the Data Act (DA) and the Digital Markets Act (DMA).

It is easy for stakeholders to get lost in this flurry of sometimes partly overlapping EU data regulations that contain a wide variety of rules about who can access what data under which conditions. This raises a fundamental regulatory design question: should data regulations be tailor-made to fit the particular circumstances of each sector or issue, or would it be better to have a single horizontal regulation with similar rules for all sectors and domains?[6] One could reformulate this question and ask if data market failures follow a general pattern across sectors, or if there are specific data market failures in some sectors or domains that merit a specific regulatory solution. To answer this, criteria are needed to assess problems in data markets and to evaluate the design of data regulations that seek to overcome these problems.

We apply the well-known economic criterion of market failure to address these questions. Regulatory intervention is justified when a market fails to operate in a socially optimal way, i.e. when it does not deliver the social welfare for society that it could potentially deliver, often because private operators have no incentive to behave in a socially optimal way. The market failures approach is recommended by the European Commission's own Better Regulation Guidelines and Toolbox[7]. Our assessment revolves around three economic characteristics of data that are at the source of most data market failures: economies of scope in the re-use of data, economies of scale and scope in data aggregation, and market incentives to invest in data collection. We examine the measures proposed in the EHDS, the DA and the DMA to overcome these market failures.

Data collection is often rival because it requires access to the physical device used by an agent at the moment of collection. Once data is collected however, it is non-rival and can be re-used for many purposes, without any functional impact on the original use for which the data was collected. Non-rivalry can generate economies of scope in the re-use of data, by the data holder and/or by a

---

[6] The tendency towards regulatory fragmentation in the digital economy has been observed before, see for instance *Solow-Niederman*, Emerging Digital Technology and the "Law of the Horse", University of California Law Review, 19.2.2019.

[7] European Commission, Better Regulation Guidelines, 3.11.2021, available at https://commission.europa.eu/system/files/2021-11/swd2021_305_en.pdf (2.5.2024); European Commission, Better Regulation Toolbox, July 2023, available at https://commission.europa.eu/system/files/2023-09/BR%20toolbox%20-%20Jul%202023%20-%20FINAL.pdf (2.5.2024).

third-party[8]. The data holder may block re-use, especially when that third party is a potential competitor to the data holder. Blocking re-use is a data market failure and may also result in a monopolistic market failure in downstream services markets.

Another and unique characteristic of data is the potential for economies of scale and scope in data aggregation or pooling[9] . These emerge when more valuable insights can be extracted from pooled data compared to fragmented datasets, when the combined social value of data exceeds their private value to individual data holders. Private entrepreneurs may create data pools by sharing the benefits from economies of scale and scope in aggregation with users who contribute their data to a pool. For example, an e-commerce platform pools data from buyers and sellers. Platform users benefit from the data pool through network effects. However, in many cases, private data markets underperform and prevent the full realisation of the social value of the data. For example, e-commerce platform data could be used to create market transparency. The platform may prevent that. Private incentives for pooling are often weak because potential participants fear losing control over their data or disagree with the distribution of benefits from the data pool. That may justify regulatory intervention to facilitate pooling and overcome private disincentives to the production of the full social value of the data.

The third market failure criterion revolves around excludability of data. Without excludability, private investment in data collection is risky because it invites free-riding by others. Excludability of non-rival products is often achieved by means of exclusive property rights for a single party, for example in intellectual property rights (IPR). In the absence of legal property rights over data , investors may apply Technical Protection Measures (TPMs) to ensure exclusive control over data and recuperate investment costs in data collection, storage and

---

[8] The concept of economies of scope was originally proposed by *Panzar/Willig*, Economies of Scope, 71(2) American Economic Review 268; *Teece*, Economies of scope and the scope of the enterprise, 1(3) Journal of economic behaviour and organization 223, 1980.

[9] For a discussion of economies of scale and scope in data, see for example: *Bajari* et al., The impact of big data on firm performance, an empirical investigation, NBER working paper nr 24334, February 2018; *Calzolari/Cheysson/Rovatti*, Machine Data: market and analytics, mimeo, European University Institute, October 2022; *Carballa-Smichowski* et al., Economies of scope in data aggregation with a case study in health data, Nov 2022.

processing. Mandatory data sharing at zero cost may erode the incentive to invest in data collection and result in a negative data supply response, unless data is a by-product of a service that is already paid for. Opening access to data through regulatory intervention therefore requires careful attention to be paid to the economic implications on the supply side. Similar to the economics of IPR, society requires a balance between exclusive monopolistic rights for investors and access and re-use rights for users. However, a major difference is that creative inventions are produced by one party, the innovator, and used by another party with different interests. Data on the other hand is co-generated between at least two parties: a data service provider and a user. Both parties may claim rights over the data but may have conflicting interests. That in itself requires a more open data governance approach.

All three EU data regulations discussed in this paper aim to overcome these data market failures by granting conditional access rights to the parties that co-generated the data, or to third parties. But they do so under very different conditions. The three data regulations span a policy spectrum from very closed, with strong control rights for private data investors and holders, to very open, with wide-ranging access rights for other co-generators and third parties, thereby facilitating the realisation of the social value of data. This paper (a) describes variations in the balance between private and social rights to data across three EU data regulations; and (b) explores if there is room to improve that balance and overcome data market failures more efficiently, ie generating more social welfare from private data. The key criterion is: can societal benefits from data be increased without undermining private incentives to invest in data collection?

Section 2 starts with the European Health Data Space (EHDS), a regulatory proposal approved by the Council and Parliament and adopted by the Parliament on 24 April 2024[10]. The reason for bringing this sector-specific data regulation to the forefront is that it ticks nearly all the data market failure boxes and solutions. It could be considered as 'best practice' in data regulation. At the other extreme of the spectrum stands the Data Act (DA), discussed in section 3. The DA is meant to be a horizontal template for 'product' data across all sectors.

---

[10] The official text of the EHDS is expected to be published in the Official Journal of the EU in the autumn of 2024. The version agreed in the Trialogue between the Council, Parliament and European Commission can be found here: https://www.consilium.europa.eu/en/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/ (26.6.2024)

But it suffers from excessive protection of data holders, giving them quasi-ownership rights to the data, at the expense of product users. It contains a mix of pro- and anti-competitive provisions, some of which may even worsen market distortions. Section 4 turns to the Digital Markets Act (DMA). This is first and foremost a competition policy tool to overcome monopolistic market failures in the services offered by very large digital gatekeeper platforms, some of which may be caused by exclusive platform control over user data. The DMA facilitates access for natural persons and business to their 'own' data. That narrow access rule may be too restrictive when data is co-generated in interactions between several parties. This paper argues that widening access to interaction data is important to level the playing field in downstream data-driven services markets. Section 5 discusses the findings.

B. Best practice in data regulation: the European Health Data Space

The EHDS ticks all the boxes in the above-described economic criteria for optimal data regulation. It facilitates the 'primary' re-use of personal health data (EHDS Article 3) and establishes the conditions for 'secondary' health data aggregation in national and EU-wide data pools (Art. 33), managed by public health authorities (Arts. 10 and 36). It puts no restrictions on primary re-use of health data at the initiative of the patient, and few restrictions on secondary re-use of aggregated health data. There are no charges for primary and secondary re-use other than the marginal cost of accessing the data (Art. 42). Charging monopolistic prices is not allowed. This pricing rule implies that all innovation benefits accrue fully to the innovator. Data suppliers cannot claim a share of the benefits.

All human health data is, by nature, personal data. The right to personal data portability, at the initiative of the data subject and at zero cost, is already foreseen in Art 20 of the EU General Data Protection Regulation (GDPR)[11]. However, in practice, the exercise of that right encounters many hurdles because the GDPR remains vague on the operational aspects of portability. The EHDS fills that gap. It defines six priority categories of health data that should be available

[11] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.

for portability: patient summaries, e-Prescriptions, medical images, medical reports, laboratory results and patient discharge reports (Art. 5). It also sets rules to operationalise real-time data portability between Electronic Health Records (EHR) systems operated by medical services supplies in the EU (Art. 6) and defines the obligations of EHR suppliers to ensure this interoperability (Arts. 17-27). In contrast to the GDPR that excludes portability of processed data, the EHDS extends portability to processed health data, for example in the form of processed medical images, medical diagnosis and treatment recommendations.

Primary health data portability is unlikely to have a negative impact on investment in health data collection. The six standardised datasets are a by-product of medical services delivery. The cost of collecting that information is already borne by the cost of medical services, paid for by patients and medical insurance providers. Doctors and hospitals will not dispense fewer medical services because the data is re-used elsewhere. There may be additional investment costs for health service providers for setting up the infrastructure for data re-use, some of it possibly borne by public health authorities. Since these six standard datasets are mandatory, service providers cannot avoid these costs. The EHDS does not contain incentives however to supply medical data beyond the standardised dataset. Additional incentives may be required for that purpose. For instance, access to digitised surgery data may require substantial investments by hospitals.

For secondary use of national health data pools for research purposes, public and private healthcare providers are obliged to make fifteen categories of data available, including the six categories of EHR data, and extending into other areas such as genetic data (Art. 33(1)). Prior private rights to these data, such as IPR and trade secrets, should be protected but cannot be invoked to withhold the data for research purposes (Art. 33(4)). Patients' privacy is protected by means of anonymised or pseudonymised access to the data (Art. 44). However, the identity of medical service providers is not protected. The EHDS imposes purpose limitations with a list of authorised and unauthorised data processing due to the sensitive nature of health data. It allows processing for health research, innovation, policymaking, regulatory and personalised medicine purposes (Art. 34). Any party with a legitimate research purpose can access the data pools. The EHDS only prohibits secondary use that would be detrimental to the welfare of patients, for example for the calculation of insurance premia, advertising or marketing activities, or the development of harmful products or services (Art. 35).

Findings from secondary use come into the public domain because researchers are required to publish the findings of their research within 18 months.

As such, the EHDS overcomes all potential health data market failures. It maximizes economies of scope in "primary" re-use of health data, and economies of scale and scope in "secondary" aggregation or pooling of health data. It also minimizes potential negative effects on data collection.

C. The Data Act: a case of regulatory failure?[12]

The DA targets "connected products" (DA Art. 2 §5 and Art 3), sometimes called Internet-of-Things devices, or data generated by tangible physical products that can communicate data outside the product. This is a new data category that did not exist before in EU data regulations. So far, the DA is the only regulation that makes this distinction. The concept of 'product' data emerged first in a 2017 European Commission Communication[13] that advocated private ownership rights over "machine" data as a means to protect industrial data. The proposed distinction between connected product and other data is rather arbitrary and confusing. Digital data does not float in thin air. All digital data requires a tangible 'product' as a physical carrier: a computer to store and process data, and an analogue-digital interface that converts digital data into analogue mechanical and audiovisual signals. These physical carriers may be located in different places, and owned and operated by different parties. The DA applies only to physical carriers that are directly handled by users.

The DA constitutes an attempt by the EU regulator to overcome monopolistic control of product manufacturers in data-driven services markets. These good intentions are enshrined in DA Art 3 §1, which grants product users direct and free-of-charge access to the product data. This enables economies of scope in the re-use of data for the purpose of producing competing or complementary data-driven services. Unfortunately, other DA provisions create obstacles for the

---

[12] A more detailed discussion of the Data Act can be found in *Martens*, Pro- and anti-competitive provisions in the proposed European Union Data Act, TILEC Discussion Paper No. 2023-03, Tilburg University, March 2023.

[13] European Commission, Communication from the Commission to the European Parliament and Council "Building a European Data Economy", 10.1.2017, COM(2017)9. The concept of data property rights was inspired by *Zech*, Information as property, JIPITEC 2015, 192.

exercise of this access right and preserve the product manufacturer's monopolistic control over the data[14].

The original European Commission DA proposal provided access to all data generated by the use of a product. This was subsequently amended to data "of the same quality as is available to the data holder". The text also distinguishes between data stored inside the product or on external servers (DA Art. 4 §1 and §2). Data transmission from a product to a server is costly. Data holders will limit retrieval to data for which they have a private business use case. This may exclude data that has value to other parties or to society at large. Modern cars for example collect thousands of data points, but car manufacturers only collect and extract business value from a few hundred of these. It is not clear if the DA would grant car users access to all data available inside their cars.

The DA restricts user access and portability to raw data only, i.e. data without any "substantial modification" or processing , beyond mere conversion of analogue signals into digital formats. This is unfair because it prevents user access to data that was processed as an explicit part of a purchase agreement and that they may have already paid for at the point of sale of the product or subscription to a related service. This provision boils down to a de-facto extension of IPR on software to the data outputs of that software . It would be equivalent to, for example, Microsoft retaining an exclusive right over processed data that is generated by Excel worksheets after users put in primary unprocessed data, and charging users when they want to transfer the processed Excel data to a third party. The contrast with the above-discussed EHDS is particularly salient here.

Apart from legal recognition of manufacturers' exclusive rights to the processed data, the DA also endorses quasi-ownership rights to unprocessed primary data. This is reflected in the provision that data holders or product manufacturers can charge third parties, when they are businesses, a price for data ported to them (DA Art. 9). That price can be based on the fixed costs as well as variable costs for data collection, storage, processing and transmission. Moreover, they can charge a monopolistic price with a mark-up margin. Only SMEs escape from monopolistic pricing (Art. 9 §4). This boils down to a licensing fee for data access, similar to a licensing fee for IPR holders. The DA tries to soften the blow by recommending a "reasonable" profit margin and Fair, Reasonable and Non-Discriminatory (FRAND) pricing (Art. 9 §1), a controversial topic in

[14] A similar point is made by *Kerber*, Governance of IoT Data: Why the EU Data Act will not fulfill its objectives, 72(2) GRUR International 120, February 2023.

standard essential patents, where FRAND pricing was first applied. While it may not be clear to economists how to calculate a FRAND price with a reasonable profit margin, the DA instructs the European Commission to set up guidelines for that calculation (Art. 9 §5).

This pricing rule is unfair because users pay twice for the data that they co-generated. At the point of sale, rental or subscription of the product, users pay the product manufacturer for the hardware and software that generates, processes and transmits primary and processed data, and possibly for additional processed data services through subscriptions. When users subsequently want to port this primary and processed data to a third party, they have to pay again for the same data. Users may want to port product data to a third-party commercial service provider to obtain competing or complementary services from that party. Although the DA states that users receive the data free of charge, the reality will be that third parties will only want to provide that service if they can charge the user for any additional costs for the acquisition of the relevant data from the original data holder.

Empirical evidence on the impact of third-party pricing rules in car maintenance, where manufacturers can charge independent maintenance service providers for access to car maintenance data, shows that it results in an increase of at least 6 percent in maintenance costs for independent service providers[15]. That distorts competition with service providers affiliated with the manufacturer . Applying FRAND pricing equally to all service providers would prevent that distortion. However, it would still result in monopolistic market failure in maintenance services.

The unequal treatment of data co-generators and the assignment of exclusive rights to product manufacturers and data holders distorts competition and slows down innovation in downstream markets for data-driven services. This constitutes a regulatory failure. We attribute this to the ghost of the 2017 European Commission Communication on data ownership rights that is still hovering over the DA, not only with the introduction of the "product data" category that comes close to "machine data", but also with the assignment of IPR-like quasi-ownership control and pricing rights to data that over-protect product manufacturers and/or data holders at the expense of users.

---

[15] *Hoegaerts/Schonenberger*, The automotive digital transformation and the economic impacts of existing data access models, report for the International Automobile Federation (FIA), 2019.

Moreover, the DA introduces further distortions in downstream data-driven product and services markets by prohibiting the use of data for competitive purposes, to compete with products and services produced by the manufacturers and/or data holders (DA Art 4 §10). The DA prohibits data transfer from data holders to third-party platforms and services that have been designated as gatekeepers under the DMA, even when requested by the product user. However, it leaves open the possibility that users transfer data directly from their device to a gatekeeper. The data architecture of the product therefore matters. If data is available on the product, users can freely choose a third-party destination, including gatekeepers. If data is stored on a cloud server operated by the data holder, transfers to gatekeepers are prohibited. For example, users of smart home appliances that store data in the cloud cannot transfer the data to their Apple or Android smartphones. That prohibition may destroy potential consumer value from interoperable components of data ecosystems. Regulators have tried to justify this prohibition with the argument that monopolistic DMA gatekeeper platforms should not be given access to even more data than they already have; it would only strengthen their market positions. The counter argument is that the DMA already imposes obligations on gatekeepers to provide users access to and portability of gatekeeper data. Data is not locked up in the gatekeeper ecosystem. The underlying problem seems to be that the DA, and the DMA, do not recognise the welfare-enhancing side of network effects and focus only on the monopolistic welfare-reducing side. That brings us to the DMA itself.

The DA also mentions trade secrets in digital data[16]. Trade secrets should not prevent access to data, other than in exceptional circumstances when the product manufacturer could suffer extreme harm. However, they "shall be disclosed only where the data holder and the user take measures to preserve their confidentiality, in particular regarding third parties." Moreover, it is up to the trade secret holder to identify the data that he considers to amount to a trade secret. It is unclear what data-related trade secrets mean in a digital context. The EU Trade Secrets Directive[17] defines three conditions that have to be met for the existence of trade secrets: (a) the information is not known either by the public

[16] On the subject of trade secrets in the Data Act, see also *Aplin*, The Data Act and trade secrets: an experiment in compulsory licensing (Chapter 6 in this volume).

[17] 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.

at large or by the experts of the sector; (b) the information has commercial value; and (c) the claimant has taken steps to keep the information secret. Following these conditions, the trade secret status of market information may vary according to the level of data aggregation. For example, data about a single sale is not a secret for the seller because the buyer has the same information. Aggregated sales data, the turnover of a seller, might constitute a trade secret for the seller, though the platform has that information too. The seller's market share on a particular platform is known to the platform operator only and cannot be a trade secret for the seller, nor for that platform. In short, data-related trade secrets will need a better definition than the Trade Secrets Directive before they can be applied in practice in the DA.

In contrast to the EHDS, the DA focuses on primary data access and portability only, i.e. the benefits from economies of scope in the re-use of data. It does not seek to generate economies of scale and scope in data aggregation, or secondary use in data pooling. The European Commission's European Strategy for Data[18] states that sectoral data pools will be the subject of separate policy initiatives. Some of these have already been launched, for example in agriculture and mobility data, though there are as of yet no details on data governance proposals for these pools.

D. Access to platform data in the Digital Markets Act

The DMA is first and foremost a competition policy instrument that seeks to reign in the anti-competitive behaviour of very large platforms that have become dominant gatekeepers because of network effects: more users make a platform more interesting to other users and therefore attract more users. More users also leave more data traces that enable a platform to improve the quality of user-matching services which, again, attracts more users. Network effects crowd out competitors and 'tip' a market towards a single dominant platform. Users then suffer from the monopolistic impact of network effects: reduced choice and increased prices may exceed user benefits from network effects. The DMA imposes obligations on gatekeepers to restrict their monopolistic behaviour, weaken

[18] European Commission, Communication for the Commission to the European Parliament and the Council, A European strategy for data, 19.2.2020, COM(2020)66 final.

network effects and stimulate competition, including through three data sharing obligations.

First, gatekeepers should give business users and end users (consumers) real-time access to the "data generated by their activities on the platform" (DMA Art. 6 §10). That enables economies of scope in the re-use of data. This obligation is an extension of GDPR rights from personal data to business user data, and from delayed to real-time access to personal data.

Second, the DMA seeks to level the information playing field between a vertically integrated gatekeeper and its business users. Gatekeepers are not allowed to make privileged use of their market data to compete with business users on their platform (Art. 6 §2). They can only use this data when they have also made it available to business users.

Third, gatekeeper search engines – in practice, Google Search – should share "query, ranking and click data" with competing search engines (Art. 6 §11). Search engines collect data on user queries and clicks on webpage rankings that the search engine delivers in response to a query. Search engines crawl billions of webpages and select and rank these to respond to queries. By observing user clicks on the proposed page rankings, they learn how to better respond. More frequently clicked pages move up the ranking. Since most queries are rare, climbing the learning curve may be slow. More users using the search engine improves data collection and delivers more efficient responses, even to rare queries. Better responses, in turn, attract even more users. User-driven and data-driven network effects explain why a single search engine became dominant.

The first two obligations suffer from lack of clarity about the extent of data sharing. User data "generated by their activities on the platform" implies access to interaction data with other users, and to processed data in the form of platform responses to user queries. For example, in an e-commerce platform, user activities necessarily entail interactions with products and services offered by sellers. What level of fine-grained market data should gatekeepers make available to competing business users, to whom should they be made available and under what conditions? To restore a market information level playing field, this should clearly go beyond business users 'own' interaction data in the platform. Some

authors[19] suggest that second-degree network interaction data should be sufficient to enable business users to position themselves more efficiently in a platform marketplace and compete with vertically integrated sellers . The third obligation for gatekeeper search engines to share query and clicks data with competitors is very far-reaching however and comprises the search engine's entire aggregated dataset, including user query inputs, search engine responses and users' clicks on these responses. It makes the full search engine data pool available to competitors.

Access to user interaction data goes beyond enabling users to benefit from economies of scope in the re-use of data. Network interaction data has a data pooling dimension across many users. Access to this data gives users access to economies of scale and scope in data aggregation. The DMA thus forces gatekeeper platforms to share the benefits from network effects with competitors, thereby levelling the data playing field between competitors. By analogy to the terms of data sharing provisions in the EHDS, this goes beyond "primary re-use" of own data and would be equivalent to "secondary re-use" of pooled data.

Regulators should be careful however with sharing of pooled data to avoid weakening network effects, because doing so may be welfare-reducing for users[20]. To the extent that Google Search's market share declines when it shares data with competitors and more competing search engines enter the market, the quality of Google Search will also decline because it collects less user data and the size of its data pool will diminish. As a result, competitors will learn less from access to Google's data, especially in the long tail of rare queries. The quality of competitor search services will not exceed the declining quality of Google Search. Consequently, the efficiency of all search engines will decline, and so will user welfare, with the weakening of data pooling and network effects. This problem could be overcome easily by replacing asymmetric data sharing from gatekeepers to competitor search engines with symmetric data sharing between all search engines, irrespective of market share. That would preserve the complete search engine data pool and thus economies of scale and scope in search data aggregation. Unfortunately, symmetric sharing is not foreseen in the DMA.

---

[19] *Martens/Parker/Petropoulos/Van Alstyne*, Towards Efficient Information Sharing in Network Markets, TILEC Discussion Paper No. DP2021-014, Tilburg University, November 2021.

[20] *Martens*, The impact of search engine data sharing on competition and consumer welfare, European Competition Journal, February 2024.

Platform data-sharing obligations are unlikely to have a negative impact on data collection because data is the by-product of platform services that are already paid for in their business models. However, the search engine case shows that the design of data-sharing rules may be important in this respect.

Moreover, like the DA, the DMA imposes FRAND data pricing but only for search engine data (Art. 6 §11). In contrast to the DA, consumers and businesses can access and transfer their 'own' data to a third party free of charge. The reason for this search engine data pricing rule is not explained but one might presume that this is meant as a – superfluous – incentive for the data holder to continue collecting data. Data collection is already incentivised by the advertising revenue that search engines generate. It gives the search data operator an exclusive quasi-licensing right on search data. It is hard to define what FRAND means in this market. Data on rare queries is more valuable than data on common queries. Smaller search engines would have higher willingness to pay for a larger dataset but less capacity to pay because of lower advertising revenue – assuming that this remains the standard search engine business model. The FRAND condition would not allow price discrimination between search engines. As discussed in the DA section, data pricing reduces data sharing and thus the welfare benefits from economies of scope in the re-use of data.

Note that the DMA does not mention trade secrets as a possible limiting factor on gatekeepers' data sharing obligations. Trade secrets are only mentioned in the context of the regulator's reporting on gatekeepers' compliance with DMA obligations.

E. Discussion and conclusions

All three EU data regulations discussed in this paper facilitate access to and re-use of data held by companies. While the EHDS puts almost no conditions on access, the DA imposes very stringent conditions, including payment of a monopolistically-priced license fee to the data holder, who becomes a quasi-owner of the data in case of third-party portability, and the prohibition on use of the data to compete with the data holder. The DMA puts no conditions on access to own platform data for natural persons and business users, but attaches quasi-exclusive ownership rights, somewhat attenuated by 'fair' pricing conditions, to search engine data.

Only the EHDS has explicit provisions for data pooling. There are none in the DA. The DMA creates some limited degree of access to market data pools by platforms. The European Strategy for Data announced that the creation of and access to sectoral data pools will be regulated in separate and still-to-be-announced policy instruments, outside the DA. Gatekeeper platforms targeted by the DMA could be considered as market data pools however. In that sense, the DMA regulates access to privately created and very large market data pools. It restricts that access to narrowly defined users' 'own' data, not to the full pool of user interaction data. Only in the case of marketplace and search engine data are platforms under the obligation to share a much wider, but not very clearly defined, interaction dataset.

All three regulations remain vague, and sometimes inconsistent, about access to processed user data. The EHDS does not distinguish between raw and processed data; it grants access to all personal health data. In the DMA, access to marketplace and search engine data also includes access to processed data. It fudges the question of whether users' access to their 'own' data includes processed user interaction data on the platform. The DA opens access to the same data as available to the product manufacturer or data holder, but then backtracks and limits access to raw or "not substantially" processed data. The EU GDPR was the first data regulation to restrict personal data access rights to raw data "contributed" by the data subject. This restriction becomes hard to maintain in the DA when processed data is part of the services related to a product that the user has already paid for at the point of sale or subscription to a service.

All three regulations frequently assert the primacy of personal data protection rules under the GDPR. However, the EHDS and DA also refer to the need to protect trade secrets. Only the DMA does not refer to that subject, at least not in the context of mandatory data sharing. It is unclear how to define trade secrets in data when data is co-generated between two or more parties.

Returning to our initial question, would one EU data regulation instrument be enough, or do we need many regulations to cover the variety of circumstances in different sectors? The comparison of the three data regulations shows that the EHDS is an example of a nearly-ideal data regulation that ticks almost all the boxes for maximum economies of scope in primary re-use and secondary economies of scale and scope in data pooling. From the point of view of overcoming data re-use market failures, it would have been a better cross-sectoral regulatory template than the DA. Applying the EHDS template for primary re-use would

have resulted in dropping the superfluous and confusing concept of product data, allowing access to processed data that users have paid for, avoiding users having to pay twice for data in the case of third-party portability, and dropping restrictions on data use for competitive purposes. Similarly, the EHDS template for primary re-use would have been a better recipe for users' access to their 'own' platform data under the DMA. It would unequivocally widen these access rights to processed direct interaction data.

The EHDS template for secondary access to data pools could also have been applied in the DMA, to give business users access to marketplace and search engine data pools. As pointed out, care should be taken to preserve the integrity of data pools in order not to weaken economies of scale and scope in data aggregation. The DMA's asymmetric data sharing obligations for search engines risk promoting competition at the expense of fragmenting that pool and thereby reducing user welfare. Symmetric data sharing, as in the EHDS, would be the preferred solution.

However, the EHDS and the DA show that it is not enough to just define access rights. They cannot be implemented without overcoming the technical obstacles to data access and portability. That requires technical standards that are likely to be specific by sector and/or domain. The EHDS and the DA pay attention to standard-setting procedures. The EHDS defines the medical dataset that should be made available. The DA covers many sectors and includes general provisions that leave room for initiatives to set data standards in various domains. The DMA still has to define standards for data sharing within and between platforms. That will require more regulatory work and instruments.

We conclude from this comparison that there is significant scope to improve data-access provisions in the Data Act and in the DMA, compared to the high standard set in the EHDS.

Chapter 3

The EU Data Act – The Interface with Competition Law

Thomas Weck*

A. Introduction

There is no general agreement on how "data" differ from "information" exactly. It is even unclear whether the word "data" has a singular, or plural – and what that would look like. But whatever data are, it is common understanding that data can be economic assets. An efficient use of such assets may give the development of the EU single market a boost. The European "Data Act" was passed into law in December 2023 with this objective in mind.[1] With the Data Act, EU Legislature seeks to enable economic actors to develop new and better products and services using data.[2]

The Data Act is going to alter certain premises on which business models were built previously. This text focuses on two chapters of the Data Act: Chapter B concerning the exclusivity and sharing of data generated by connected products, and Chapter C concerning the switching between data processing services.

---

* Prof. Dr. Thomas Weck, LL.M., Associate Professor of Public Law, Regulatory Law and Comparative Law at Frankfurt Competence Centre for German and Global Regulation (FCCR) of Frankfurt a.M. School of Finance and Management, Germany, t.weck@fs.de. I declare that the FCCR in receives regular funding by Google, AWS and other companies although it is independent vis-à-vis funding partners.

[1] Regulation (EU) 2023/2854 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, 2023/2854, 22.12.2023, p. 1-71.

[2] Data Act, recitals 1 and 2.

B. Data exclusivity and data sharing

The Data Act regulates access to data for 2 different reasons: On the one hand, it aims for a practical solution to the problem of who is entitled to use machine-generated data.[3] On the other hand, it regulates data sharing in the public interest.[4] This text focuses on the first aspect.

I. Machine-generated data as co-generated data

Machine-generated data are frequently co-generated. The parties involved in the generation of the data are the manufacturer of a device, and its professional or private operators. We may think of an aircraft operated by an airline, or a car operated by a consumer. In these scenarios, the interest in accessing data generated by the device may give rise to conflicts. The professional or private operators of devices may want to access machine-generated data in their own interest. But it is the manufacturer that controls the design of the device. The manufacturer, thus, also controls access to the data which the device generates, and the manufacturer may not have an interest in sharing the data.[5]

II. Data access obligations in existing law

Thus, the question arises: Why not simply impose a data sharing obligation? In fact, there are data sharing obligations even in existing law. However, those obligations are rare. This is because the decision to grant others access to data, or other assets is generally based on the freedom of contract.

It is true that this freedom has its limitations, which exist in the public interest. When it comes to the interest of protecting market entry, the so-called essential facility doctrine may apply.[6] Under the essential facility doctrine, market-

---

[3] Art. 3-13 Data Act and recitals 2, 4-6 ("horizontal rules").

[4] Art. 14-22 Data Act and recitals 5, 63 ff.

[5] The manufacturer may at least not be willing to share data that can be used to harm the manufacturer's own interests, e.g., data used to design competing devices or to hold the manufacturer liable in case of malfunctioning; in this context, see also Art. 4(10), 5(6) Data Act.

[6] CJEU (ECJ), Judgment of 12.05.2022, Servizio Elettrico Nazionale, C-377/20, ECLI:EU:C:2022:379, para. 83; Judgment of 26 November 1998, Bronner, C-7/97, EU:C:1998:569, paras. 41, 44 ff.; Judgment of 06.04.1995, RTE and ITP ("Magill"), C-241/91 P, ECLI:EU:C:1995:98, paras. 53 ff.; Judgment of 29.04.2004, IMS Health, C-

dominant firms must provide access to data or other assets under two conditions: One is that the assets operate as a non-duplicable input to offerings downstream; and the second is that without access, competition downstream would be eliminated.[7] In addition, regulation can be used to lower the bar for access if other public interests than the interest in market entry call for it.[8]

Regulation plays an important role when it comes to forcing access to assets such as network infrastructures. When it comes to data, regulation imposes access obligations, e.g., for data used for R&D, statistical, or tax purposes. Moreover, public data are more open to access than private data.[9] However, there is no law forcing access to machine-generated data as such.

This is not by accident: In fact, mandatory data sharing can undermine the business interests of manufacturers in the collection of data. This would run counter to the policy interest in the development of a data-driven economy. Thus, the pre-existing state of the law had some merit when it comes to ensuring the free development of markets.

III. Reasons for changing the law

However, the arguments in favor of leaving data access to the freedom of contract do not provide the complete picture. In fact, complaints have multiplied

---

418/01, ECLI:EU:C:2004:257, para. 38; *Graux*, Sharing Data (Anti-)Competitively, data.europa.eu, 2022, p. 9. See *Kerber/Eckardt*, Designing the Bundle of Rights on IoT Data: The EU Data Act, Section C (Chapter 1 in this volume), and *Martens*, A comparative economic perspective on EU data market regulations, (Chapter 2 in this volume).

[7] CJEU (ECJ), Judgment of 12.05.2022, Servizio Elettrico Nazionale, C-377/20, ECLI:EU:C:2022:379, para. 83; Judgment of 29.04.2004, IMS Health, C-418/01, ECLI:EU:C:2004:257, paras. 38, 47; Judgment of 26.11.1998, Bronner, C-7/97, ECLI:EU:C:1998:569, para. 41; see also CJEU (ECJ), Judgement of 12.01.2023, Lietuvos geležinkeliai, C-42/21 P, para. 79.

[8] CJEU (GC), Judgment of 18.11.2020, Lietuvos geležinkeliai/Commission, T-814/17, ECLI:EU:T:2020:545, para. 92.

[9] See Art. 42 of the Charter of Fundamental Rights and *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, Study for the European Parliament, PE 732.266, May 2022, p. 39-40 as well as the EU legislation referred to there; §§ 30 Abs. 4 AO; 16 (6) BStatG; §§ 1, 4 DNG; § 12a EGovG; § 1 Abs. 1 IFG, § 3 UIG, § 2 Abs. 1 S. 1 VIG in German Law. See further *Falkhofen*, Infrastrukturrecht des digitalen Raums, EuZW 2021, 787 (789-790).

in recent years that collected data are under-utilized.[10] These complaints have some merit, too: If we look at things from the perspective of those who do not have access to machine-generated data, we notice that a shared use of such data might allow for the development of additional products or services.[11]

But markets for such other products or services do not develop easily – even where demand exists. One reason may be that device manufacturers exercise exclusive control of devices generating data, and that they do not have their own interest in sharing the data.[12] Another reason may be that the legal rights in co-generated data are somewhat unclear.[13] This makes it difficult for those not exercising factual control to assert their rights in the data.

At the same time, we notice that machine-generated data are frequently not the core of the business of device manufacturers: An aircraft or car manufacturer will not stop to design and produce airplanes or cars simply because it must share the data generated with these devices. Thus, mandatory data sharing is unlikely to disrupt the manufacturers' businesses.

IV. Data access and data sharing under the Data Act

Following what was said before, arguments exist that regulated data access and data sharing may contribute more effectively to the market development than leaving data access and data sharing to private negotiations based on the freedom of contract.[14]

This is where the Data Act comes into play. Art. 4 of the Data Act obliges data holders controlling the technical design of so-called "connected products" to share the data generated by those products with others. This obligation covers

---

[10] European Commission, 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), 23.2.2022, SWD(2022) 34 final, p. 7-8; OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, 2019, https://doi.org/10.1787/276aaca8-en, p. 17 ff.

[11] OECD, ibid., p. 62-64, 65 ff.

[12] See European Commission, Data sharing and competition law, 5.5.2023, section: Market competition and data, available at https://data.europa.eu/en/publications/datastories/data-sharing-and-competition-law (2.5.2024).

[13] Cf. Data Act, recital 2.

[14] See *Metzger*, Contracts under the Data Act: Review of standard terms and FRAND conditions (Chapter 5 in this volume), on an assessment of the Data Act from a contract-law perspective.

raw data and related metadata.[15] The data must be machine-readable, but no requirements exist that they are in a format allowing for specific use by other parties.[16] Moreover, the access obligation does not cover information derived from the processing of data with complex algorithms, or the algorithms to process data themselves.[17] Thus, the data holder does not have to make additional investments, or be afraid of losing its investments in tools to make use of data.

However, this is not the full story. Additional complexity arises because access to co-generated data may be claimed in situations where there are third-party rights or interests. These third-party rights or interests may effectively thwart the access claim. This issue is well-known from essential facility claims.[18] Two scenarios may be distinguished:

- One scenario exists where the commercial operator of a connected product, let's say, an airline company, asks a plane manufacturer for data access, and the pilots or airline clients raise data protection concerns.
- A second scenario would be if consumers or suppliers of additional consumer products or services ask for data access; let's say where consumers bring their car to the repair shop. Here, the car manufacturer may itself raise concerns – not data protection concerns, but concerns of trade secret protection.

In its treatment of third-party rights potentially hampering data access and data sharing, the Data Act introduces some novelties: First of all, the Data Act neutralizes data protection issues in cases where entrepreneurs want to obtain access to data from a connected device operated by a consumer. This is because it's not third-party businesses interested in the access, but the users of the connected devices that will be empowered to claim access or share data for defined purposes under Arts. 4 and 5 of the Data Act.[19]

---

[15] See Art. 4(1) and recitals 15, 20 of the Data Act.

[16] Cf. Art. 4(1), 3(2)(a) Data Act.

[17] Recital 15 of the Data Act.

[18] *Federle/Asbroeck*, Data Access Claims Under Competition Law and Data Privacy Requirements, Concurrences 2020; *Dacar*, Is the essential facilities doctrine fit for access to data cases? The data protection aspect, 18 CYELP 61, 2022; *Weck/Reinhold*, Data-related abuses under European law, 5 Bus. Econ. L. Rev. 136, 2021, available at: https://scjg.cnki.net/kcms/detail/detail.aspx?filename=JMFV202105010&dbcode=CJFQ&dbname=CJFDTEMP&v (2.5.2024).

[19] Art. 4(1), 5(1) Data Act.

However, the Data Act does not change the rules that are otherwise applicable in the relationship between data holders and users (or indirectly affected GDPR[20] right holders).[21] Thus, an access claim will not be successful where there is a discrepancy of interests between the access claimant and users (or indirectly affected GDPR right holders). It is not to be expected, for instance, that an insurance carrier can ask for data about a consumer's driving habits, without the consumer itself taking the initiative.

Whereas the Data Act somewhat strengthens the position of consumers, the trade secrets of data holders will be pushed back, as an obstacle to data sharing. Indeed, since we are talking of co-generated data, trade secrets can generally only be recognized for the data holder's own added value. The Data Act limits reliance on trade secrets in several provisions in Arts. 4-6.[22] The rule is that trade secrets cannot be used to block data access completely, but access claimants may have to use all proportionate means to protect the interests of the trade secret holder. These rules were highly controversial in trilogue, before formal legislation.[23]

However, feedback from the industry suggests that the actual relevance of trade secrets may be limited in the regulated scenarios. Indeed, the knowledge of raw and meta data alone will often not be enough to appropriate the added value provided by the data holder, e.g., the manufacturer of a connected device. Moreover, other parties will request data access or data sharing usually out of an interest in complementary products or services. In contrast, their interest will not relate to competing products or services.[24] Consequently, some manufacturers

---

[20] GDPR = Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.

[21] See Art. 4(10)-(12), 5(7) Data Act. See *Sattler*, Data Act and Data Protection Law (Chapter 7 of this volume), in more detail.

[22] Art. 4(6)-(9), 5(9)-(12) Data Act.

[23] *Bertuzzi*, EU policymakers inch toward deal on trade secrets in new data law, Euractiv of 8. Juni 2023; *Zech*, Data Access Rights as Property Rights, Section B.II (Chapter 4 in this volume), and *Raue*, »Without prejudice«: The Interface of the Data Act and Copyright, Section A (Chapter 8 in this volume).

[24] See Art. 4(10) Data Act protecting the use of relevant data to develop competing products. Note that Art. 5(6) Data Act is a corresponding provision protecting the competitive interests of third parties.

even support the Data Act, hoping that the prospective complementary products or services will provide their customers with additional benefits.

In addition, the following note may be added from a competition lawyer's perspective: The Data Act will not provide the only directly applicable rules when it comes to trade secrets. In addition, Art. 101 TFEU prohibits deliberate disclosure of strategic information, incl. trade secrets, among competitors.[25] This rule also applies if the mutual disclosure takes place via the customers. In this context, however, it is an objective obligation and not a subjective right of manufacturers to keep their trade secrets for themselves.

C. Data infrastructures and data portability

The Data Act not only regulates access to data, but also data infrastructures. With the Data Act included, EU regulation covers two types of data infrastructures: Private infrastructures, where the relevant rules are scattered across the Free Flow of Data Regulation (FFDR), the Data Act, and the Digital Markets Act (DMA), and public infrastructures, which will be regulated by the FFDR and the Data Governance Act.[26] More specifically, Chapter VI of the Data Act concerns the switching between data processing services and the porting of data.

I. CSP as relevant norm addressees

This text only covers private infrastructures. These private infrastructures can be established for the sharing of data (data marketplaces) or data storage. The latter notably include the infrastructures of cloud service providers – or

[25] See European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements, OJ C 259, 21.7.2023, p. 1-125, paras. 373 ff.

[26] In addition to the reference in fn. 1, see Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59-68; Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1-66; Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1-44.

"CSP".[27] CSP allow for data storage and may offer specific services for the processing of stored data. They have developed as stand-alone business or as parts of digital ecosystems.[28] For instance, Amazon, Apple, Microsoft, and Google all offer cloud services.

These digital ecosystems operate both as market participants and as rulesetters for other market participants using their services.[29] They may be built around so-called "core platform services" and have shielded themselves from outside competitive advances.[30] This gives rise to particular competition issues, which are now regulated by the Digital Markets Act. Although this regulation is not in our focus here, it must be taken into account when we talk about cloud services.

II. Market trends and need for regulation (?)

The development of cloud services has been determined by two opposing trends in recent years.[31] These are general trends, but they also affect services to CSP customers. On the one hand, we see a modularization of software and a decoupling of software functionalities. Software functions are being outsourced and provided as a single-purpose micro-services through an interface. Customers, thus, find specialized services on the market which they can put together according to their individual needs.

On the other hand, we have been witnessing concentration tendencies around intermediaries. Regarding CSP services, the offer of a simple data storage service may be bundled with online market places for customized products and services, or benefit from being embedded in a digital ecosystem built around an

---

[27] Cf. Data Act, recital 78.

[28] See Digital Markets Act, recitals 3, 32; Monopolies Commission, Special Report 82: Recommendations for an effective and efficient Digital Markets Act, 1st ed., Oct. 2021, paras. 28 ff. on the digital ecosystem concept.

[29] *Crémer/de Montjoye/Schweitzer*, Competition policy for the digital era, Final Report for the EU Commission, 2019, p. 60 ff.

[30] Digital Markets Act, recitals 2-3.

[31] See, e.g., *Giustiziero* et al., Hyperspecialization and hyperscaling: A resource-based theory of the digital firm, 44 Stategic Management Journal 1391 (1414 ff.), 2023; *Sturgeon*, Upgrading strategies for the digital economy, 11 Global Strategy Journal 34 (41 ff.), 2021, which lists procompetitive pooling as a potential third trend.

economic platform. In both instances, the operator benefits from network effects, i.e., additional users render the service more and more attractive.

The trend towards comes along with its own benefits: A single organization is oftentimes more efficient in providing service than several organizations working together. Moreover, large service providers can establish industry standards most easily. However, centralized standardization codifies the status quo, which is not always good.

In any case, we see that the market is evolving. Hence, is there a need for regulation? On the one hand, the modularization trend facilitates market entry for both basic storage services and individualized processing services. However, modularization leaves less scope to individual service providers for the creation of added value. On the other hand, the concentration trend is certainly unlikely to seclude markets for basic storage. That being said, it may contribute to the permanent tipping of linked platform markets. This may contribute to the unassailability of digital ecosystems and may be problematic. Thus, in support of current EU regulation, we may acknowledge that safeguards are necessary to keep markets dynamic.

III. Asymmetrical regulation vis-à-vis DMA-designated CSPs

The EU legislator has opted for an asymmetrical approach towards regulation of CSP, at least to the extent that they form part of large digital ecosystems. This approach pervades EU regulation beyond the specific switching rules of the Data Act.

In the Digital Markets Act, Legislature has imposed positive data access obligations on large digital ecosystem operators – which it calls "gatekeepers". This was done, among other things, to prevent the gatekeepers from self-preferencing.[32] The Data Act, in turn, blocks access to data for "gatekeepers" in terms of the DMA.[33]

However, access claims under the Data Act will not be caused by gatekeepers pursuing a self-preferencing interest. They will rather be made by users of connected devices out of their own interest. This raises the question whether the

---

[32] Art. 6(8)-(11) DMA.

[33] Art. 5(3), Art. 6(2)(d) Data Act; see *Bueren/Weck* in: Münchener Kommentar Wettbewerbsrecht, Band 1, 4th ed. 2023, DMA, Art. 5 para. 69, Art. 6 paras. 205, 228.

restrictions in the Data Act have a valid foundation from a competition-policy perspective.

IV. "Functional equivalence" to facilitate switching between CSPs

Another important feature of the new regulation is that it strives to facilitate the switching between CSP services. The Digital Markets Act imposes "data portability obligations". With these obligations, it aims to address the lock-in of private users of gatekeeper services.[34] The background is that once users have opted for the services provided in a digital ecosystem, they may find it difficult, or may lose their interest to switch to competing services.

Regulation dealing with consumer lock-ins is getting more and more important, also in other areas. The interest to overcome consumer lock-in is behind, for instance, a data portability provision in the GDPR as well as EU regulations against geo-blocking and enabling the portability of online content.[35] It is also relevant where financial market rules allow consumers to switch with their account to another bank without service disruption.[36] Likewise, it is relevant where telecom rules allow consumers to switch to another telecom provider without having to give up their phone number.[37]

The Data Act will introduce a new concept to facilitate the switching of users. In this case, however, the rules will apply to CSP regardless of whether they form part of a digital ecosystem. Moreover, the aim is to facilitate primarily the

---

[34] Cf. Art. 6(9) DMA.

[35] Art. 20 GDPR; see, additionally, Regulation (EU) 2018/302 of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, OJ L 60I , 2.3.2018, p. 1-15; Regulation (EU) 2017/1128 of 14 June 2017 on cross-border portability of online content services in the internal market, OJ L 168, 30.6.2017, p. 1-11.

[36] Art. 9 ff. Directive 2014/92/EU of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, OJ L 257, 28.8.2014, p. 214-246; in German law: §§ 20 ff. ZKG.

[37] Art. 5(1)(d), 106 and recitals 278 ff. of Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, p. 36-214; in German law: § 59 TKG 2021 and *Kühling/Bulowski/Schall*, Telekommunikationsrecht, 3rd ed. 2023, § 3 paras. 97 ff., especially paras. 104 ff.

switching of business users. CSP will be required to ensure so-called "functional equivalence" of their own and target CSP services.[38]

It has been said that "functional equivalence" was derived from telecommunications regulation. Telecommunications regulation requires network operators with significant market power to ensure equivalence of input and output regarding network access.[39] However, the obligations in telecommunications regulation concern services controlled by telecommunications network operators. They are imposed to prevent discrimination in the vertical relationship between the respective operator and network customers in the operator's own favor (self-preferencing). In contrast, the CSP stand in a horizontal relationship with third-party CSP and do not control data the infrastructures of these CSP. Thus, drawing a parallel between the situation in telecommunications networks and in the cloud context is problematic.

In any event, the majority of business customers of CSP multi-home, and basic CSP services are substitutable. Moreover, target CSP have their own interest to facilitate switching by business customers to the extent possible. Thus, it is also the question whether the basic assumption of the functional equivalence provisions in the Data Act is correct: That the situations covered by the Digital Markets Act and the Data Act are sufficiently comparable to justify the transfer of the DMA's portability concepts from consumer-oriented regulation to regulation dealing with business users. Be this as it may, it is no wonder that the new rules proposed in the Data Act have been very controversial so far.

D. Conclusion

To conclude: The Data Act departs from existing legal concepts in order to enable the use of data and, thereby, to contribute to the EU single market. Its rules concerning data access and data sharing may in fact solve an existing issue: The inertia of manufacturers when it comes to allowing others to use co-generated data. In contrast, the rules concerning data infrastructures, such as cloud services, raise a number of questions because they are not based on clear concerns such as, e.g., self-preferencing concerns.

---

[38] Art. 23 ff. Data Act.

[39] This also covers services depending on such access; see Art. 70(2), 78(1), Art. 81(2) subpara. 1 and recitals 185, 200 ECEC; in German law, especially § 24(2) TKG.

Part II

Legal Foundations

Chapter 4

Data Access Rights as Property Rights

Herbert Zech*

Property rights theory is still an important and useful analytical framework to understand the mechanism of data sharing. Although, with the advent of the Data Act, the focus has changed from data ownership to data access, the question remains whether and how the future legal framework will facilitate data contracts. This article is based on the premise that functioning data markets are a key aspect for intensifying data use, especially for the training of AI (although, also with data, arguably, as with any good, there is an optimum level and an increase in data use is not an end in itself, only the optimum use of data). Therefore, based on property rights theory, this article examines whether the Data Act has the potential to enable data markets.

The article proceeds (after preliminary remarks on the property rights theory and on the Data Act's data sharing mechanism) by analysing first the position of the data holders, second the position of the users, and finally asking the question if the position of both can be seen as a kind of co-ownership or can be contractually treated as such. This bears in mind that also the production of the data is a kind of joint effort, an aspect which is also explicitly stated in Recital 6 of the Data Act.[1]

---

* Prof. Dr. Herbert Zech, Chair of Civil Law, Technology Law and IT Law at Humboldt University, Berlin, Director at the Weizenbaum Institute. This article will also be published in Lohsse/Schulze/Staudenmayer (eds.), Private Law and the Data Act (forthcoming).

[1] Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), OJ L 2023/2854, 22.12.2023, p. 1-71, Recital 6 sentence 1: „Data generation is the result of the actions of at least two actors, in particular the designer or manufacturer of a connected product, who may in many cases also be a provider of related services, and the user of the connected product or related service."

The article itself and its structure builds on a paper by Martina Eckardt and Wolfgang Kerber[2]. Their paper discusses to which extent different concepts of data governance are realised in the Data Act. First, it shows that the Data Act builds, as a starting point, on a data holder-centric concept, assigning the bundle of rights on non-personal IoT data in an IP-like way to the data holders. Second, it shows how the Data Act adds a user-centric concept, assigning the bundle of rights on non-personal IoT data to the users (which arguably are the lynchpin of the data markets facilitated by the Data Act). Finally, the article discusses the concept of co-generated data, going beyond exclusivity, as the most suitable concept for IoT data markets (also advocated by other important voices in academic literature[3]).

A. Preliminary Remarks

I. Property Rights

Property rights theory provides a theoretical framework for the legal attribution of goods. By explaining the economic function of such an attribution, i.e. facilitating markets, it provides one potential justification of such rights. The archetype of such an attribution is ownership, comprising the exclusive right to use and to transfer this position. However, even legal ownership comes with restrictions. IP rights still provide for exclusivity but feature broader exceptions and limitations. Although property rights theory defines such rights as a bundle of rights (and privileges), this can be reconciled with the Blackstonian view of things as objects of property. Whether you stress one aspect or the other is „largely a matter of focus" (Merrill/Smith).[4] So the answer to: "What is ownership? Is there such a thing as ownership in a thing or has it to be understood as

---

[2] *Eckardt/Kerber*, Property rights theory, bundles of rights on IoT data, and the Data Act, 57(1-2) European Journal of Law and Economics 113, 2023. See also *Eckardt/Kerber*, Designing the Bundle of Rights on IoT Data: The EU Data Act (Chapter 1 in this volume).

[3] ALI/ELI Principles for a Data Economy, Data Transactions and Data Rights, As Adopted and Promulgated by The American Law Institute on May 18, 2021 and The European Law Institute on September 1, 2021 (Principles 18-23); *Metzger/Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42 (55).

[4] *Merrill/Smith*, Property, 2010, p. 6; similar *Zech*, Information als Schutzgegenstand, 2012, p. 100-102.

nearly a bundle of entitlements to that thing?" is that current legal research sees it as a kind of spectrum.

Characterising the different aspects of the bundle of rights allows the analysis of existing legal rights. As such aspects in relation to things or goods can be differentiated: rights to exclude, use, and transfer. These three aspects have been called the „core of property".[5] An older categorisation, found in property rights theory, differentiates *usus* (use), *usus fructus* (enjoyment of fruits of the use), *abusus* (misuse) and *translatio* (transfer).[6] For information goods, like raw data, this can be reinterpreted to access, use, integrity, and transfer.[7] From an economic perspective, information goods are non-rivalrous in their use. Therefore, access (which may be exclusive or non-exclusive) replaces possession (which is exclusive).[8] Access enables the use of information. However, exclusivity, use, and transfer remain the core aspects of property.

An important aspect of typical property rights, like ownership and IP, is that they are „good against the world"[9], they have, legally speaking, an in-rem effect (as opposed to an in-personam effect). Property rights theory is not limited to legal attribution. In contrast, it accepts, from an economic point of view, any kind of attribution facilitating the contractual exchange of goods as equal. Such an attribution may be legally protected, based on any social guarantee for an expectation, or only factually protected.[10] The key aspect is that the attribution must be transferable. Therefore, assignable IP rights qualify as property rights whereas personality rights only contain some aspects of property (allowing for the licensing of personality aspects) but in their core are not property rights.[11]

---

[5] *Merrill/Smith*, Property, 2010, p. 6.

[6] *Zech*, Information als Schutzgegenstand, 2012, p. 116.

[7] *Zech*, Information als Schutzgegenstand, 2012, p. 117-129; *Zech*, Information as Property, JIPITEC 2015, 192 (195).

[8] *Zech*, Information as Property, JIPITEC 2015, 192 (195); *Zech*, Data as a tradeable commodity, in: De Franceschi (ed.), New Features of European Contract Law – Towards a Digital Single Market, Intersentia, Cambridge, 2016, p. 51 (56).

[9] *Merrill/Smith*, Property, 2010, p. 9.

[10] *Barzel/Allen*, Economic Analysis of Property Rights, 3rd ed. 2023, p. 15-19; cf. *Merrill/Smith*, Property, 2010, p. 2.

[11] *Sattler*, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 GDPR, in: Lohsse/Schulze/Staudenmayer (eds.), Data as Counter-Performance – Contract Law 2.0, 2020, p. 225 (244s.: "personal data can be traded, but not transferred").

The economic analysis of property rights focuses on their function of facilitating contracts. However, they might have other important economic functions (and hence, from a legal policy point of view, justifications) like incentives to invest. Nevertheless, property rights always focus on goods and their attribution as a basis for trading these goods. To sum it up, the important questions when analysing a legal position are: "Can I exclude others from the use of these goods, can I use the goods myself, and finally, can I transfer that position?"

A final interesting aspect of property rights is that property law is also seen as a basis for corporate law (alongside contract law).[12] Whereas corporations are based on multilateral contracts, their functioning in the markets can only be explained with the additional in-rem effects of property rights regarding their assets.

II. The Data Act data sharing mechanism

Before beginning with the detailed analysis of the positions of the data holder and the user, the data sharing mechanism provided by the Data Act (especially Articles 4 and 5) shall be briefly introduced. The mechanism mainly concerns a triangle between data holders, users, and data recipients (defined in Article 2(13), (12) and (14) respectively). The Data Act stipulates an accessibility obligation (Article 3 DA) and an access right (Article 4 DA), making available product data and related service data to the user of the connected product or related service (cf. Article 1(1)(a) DA), and a sharing right (Article 5 DA), making available data by data holders to data recipients (cf. Article 1(1)(b) DA). According to Article 4(1) DA, data holders shall make certain data accessible to the user (access right). According to Article 5(1) DA the data holder shall, upon request by a user, make certain data available to a third party without undue delay (sharing right). Article 5(1) DA explicitly states that this shall be done in accordance with Articles 8 (agreement between data holder and third party) and 9 (compensation based on this agreement) but free of charge to the user.

---

[12] *Hansmann/Kraakman*, Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights, 31 J. Leg. Stud. 373, 2002; *Armour/Whincop*, The Proprietary Foundations of Corporate Law, 27 Oxf. J. Leg. Stud. 429, 2007; cf. *Armour/Hansmann/Kraakman/Pargendler*, What is corporate law?, in: Kraakman et al. (eds.), The Anatomy of Corporate Law, 3rd ed. 2017, p. 1 (5-6).

Regarding the legal policy functions of these rules, Recital 2 DA states „an optimal allocation of data for the benefit of society" as the aim of the data sharing mechanism. Recital 32 DA refers to the overarching aim of this optimized data use: „not only to foster the development of new, innovative connected products or related services, stimulate innovation on aftermarkets, but also to stimulate the development of entirely novel services making use of the data concerned, including based on data from a variety of connected products or related services." On the other hand, Recital 32 DA also shows the conflict with welfare-relevant interests of the data holders: „At the same time, this Regulation aims to avoid undermining the investment incentives for the type of connected product from which the data are obtained...". As a consequence, the Data Act tries to strike a tricky balance between a better allocation and, consequently, a better use of data on the one hand, and avoiding disincentives for the data holders (for whom constructing new IoT-devices might become unattractive) on the other hand.

B. The position of the data holder

The position of the data holder shows two important aspects: de facto control of the data, arguably linked with trade secret protection, and the requirement of a contract with the user.

I. De facto control of the data

The Data Act, as a starting point, acknowledges the data holders' control over "their" data. Data holders are allowed to keep their de facto control over the data, although with the important exception of Article 3 DA (obligation to make product data and related service data accessible to the user). They are even allowed to use technical protection methods, Article 11(1) DA.

II. Trade secret protection

Arguably, data holders also enjoy trade secret protection. Articles 4 and 5 DA may even be seen as a model for compulsory licences in trade secrets, where complex rules try to maintain the trade secret while at the same time granting access to certain entitled parties.

The key requirement for trade secret protection is that the data can be qualified as information in the sense of Article 2(1) Trade Secrets Directive (TSD).[13] In addition, the information must be secret (lit. a), have commercial value because it is secret (lit. b), and be subject to reasonable steps to keep it secret (lit. c). Among these requirements, arguably only commercial value may be interpreted in a way allowing the restriction of protection for raw data.

Information in the sense of Article 2(1) TSD must be understood as semantic information (meaning it is demarcated on the semantic level).[14] This, however, does not rule out the protection of data sets or even a single datum. Trade secret protection has an effect on any embodiment of the protected information, meaning any representation by code (on the syntactic level) or physical embodiment on a data carrier (on the structural level). Data in the sense of the Data Act is a digital representation of information. According to Article 2(1) DA "'data' means 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". Recital 15 DA distinguishes data in raw form (source or primary data), pre-processed data, and information inferred or derived from such data. All of them are information in the sense of the Trade Secrets Directive. Although, in the Data Act, the data sharing mechanism only encompasses data in raw form and pre-processed data and the term information is only mentioned with the information inferred from such data, this does not change the assessment of the term information in the Trade Secrets Directive.

The remaining valve is the requirement of a commercial value. It may be argued that single data do not have a significant value. However, the fact that there is an unmet demand for raw data shows that data do have a value, even if only a very small one per single datum. It may also be argued that judging the value from the perspective of the trade secret (data) holder leads to a lack of commercial value. Recital 14 TSD links the commercial value to the harm for the trade

---

[13] *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, p. 59 (65-66); *Zech*, A legal framework for a data economy in the European Digital Single Market: rights to use data, 11 JIPLP 460 (465), 2016; *Zech*, Data as a tradeable commodity, in: De Franceschi (ed.), New Features of European Contract Law – Towards a Digital Single Market, 2016, p. 51 (62-62).

[14] *Zech*, Data as a tradeable commodity, in: De Franceschi (ed.), New Features of European Contract Law – Towards a Digital Single Market, 2016, p. 51 (62).

secret holder caused by unlawful acquisition.[15] However, even from this perspective, the loss of the possibility to trade the data means a harm for the trade secret holder. To sum it up, regardless of how small the value of a single datum may be, data sets or raw data in general do have a commercial value, although mostly a small one.[16]

Although Recital 16 TSD stresses that the Trades Secrets Directive "should not create any exclusive right to know-how or information protected as trade secrets", Trade Secret Protection resembles in many aspects IP rights (e.g. regarding enforcement and licensing (from a competition law perspective, TT-BER)).[17] Not least, it enjoys protection as property under the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

The Data Act seems to be ambiguous about whether raw data may be protected as trade secrets. Recital 20 DA seems to deny the existence of exclusive rights in data: „manufacturers are able to determine, through their control of the technical design of the connected products or related services, what data are generated and how they can be accessed, *despite having no legal right to those data*"[18]. This may be explained by the qualification of trade secret protection as not being an exclusive right (Article 43 DA ensures that the right for the maker of a database in Article 7 of Directive 96/9/EC does not apply). Recital 31 DA, on the other hand, acknowledges at least the possibility of trade secret protection: "While this Regulation requires data holders to disclose certain data to users, or third parties of a user's choice, even when such data qualify for protection as trade secrets, it should be interpreted in such a manner as to preserve the protection afforded to trade secrets under Directive (EU) 2016/943." This wording seems to leave the question whether trade secret protection for raw data is possible open.

---

[15] Cf. *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, p. 59 (65).

[16] *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, p. 59 (66).

[17] Cf. *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, p. 59 (64): "Trade Secrets Directive precludes rights *in rem*".

[18] Emphasis added.

Arguably, trade secret protection is part of the balance between the interests of the data holders and the interests of the parties entitled to access the data. Trade secrets are preserved under the Data Act (meaning that it does not follow an open data approach). This is not only expressed in Recital 13 DA but also in Article 8(6) DA which states that "[u]nless otherwise provided for in Union law, including Article 4(6) and Article 5(9) of this Regulation, or by national legislation adopted in accordance with Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets."

The Data Act contains detailed rules for the preservation of trade secrets in Article 4(6)-(9) DA and Article 5(9)-(12) DA: Trade secrets shall only be disclosed where the data holder and the user take all necessary measures to preserve their confidentiality. Confidentiality agreements between holder and user or holder and recipient are envisaged. In exceptional circumstances the holder may refuse. An elaborate dispute settlement mechanism and a right to seek redress are stipulated.

III. Use and transfer: requirement of a contract with the user

While data holders do enjoy factual and even legal (trade secrets) protection, they are not free to do with the data whatever they want. In contrast, Article 4(13) and (14) DA stipulate for non-personal data the need for a contractual agreement with the users if they want to make use of the data or if they want to transfer the data. For personal data, a similar restriction arises from data protection where consent given by the data subject (Article 4(1) GDPR) according to Article 6(1)(a) GDPR arguably serves as the main (but not the only one) potential reason for the lawfulness of processing.[19]

This amounts to a kind of exclusive right for the users relative to the holders (which shall be examined in more detail under III.). Two aspects may be discerned: use and transfer.

Use is addressed in Article 4(13) DA. Article 4(13) DA requires for all readily available non-personal data a contract with the user: "A data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user". This means that the right to use the data is allocated with the user.

---

[19] *Sattler*, Data Act and data protection law (Chapter 7 in this volume).

Transfer is addressed in two different rules, Article 4(14) DA and Article 8(4) DA. Article 4(14) DA only applies to non-personal product data (data generated by the use of a connected product, Article 2(15) DA): "Data holders shall not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them." This means that the right to transfer non-personal product data is also allocated with the user. A similar rule can be found in Article 8(4) DA: "A data holder shall not make data available to a data recipient, including on an exclusive basis, unless requested to do so by the user under Chapter II." However, this rule arguably applies to all kind of data. As a parallel to Article 4(13) DA, the rule might be understood to be restricted to non-personal data with personal data following GDPR.

As a summary of the position of the data holder, trade secret protection is preserved regarding third parties but the rights to use and transfer data are allocated with the user. The holder keeps the possibility to exclude third parties (meaning parties that are neither user nor data recipients). But the right to use non-personal data is allocated to the user (the right to use personal data according to the GDPR to the data subject). Moreover, the right to transfer is also allocated to the user.

C. The position of the user

Users enjoy (besides being the beneficiaries of the accessibility obligation according to Article 3 DA) the access right according to Article 4 DA and the sharing right according to Article 5 DA. In addition, as was already shown, with respect to the holders, the use is assigned to the users which, together with trade secret protection, amounts to an exclusive use right (see at 2.). This position is also transferable (see at 3.).

I. Use/access

Access factually enables the use of the data.[20] The possibility to use is therefore mediated by the right to access. Access is also facilitated by the accessibility obligation in Article 3 DA. The right to access the data is stipulated in Article 4 DA (rights and obligations of users and data holders with regard to access). This right is transferable by virtue of Article 5 (right of the user to share data with third parties). To be precise, the access right is not transferable as such, but another right of the user is created (the sharing right) which entails the access and use by the recipient. This may be the reason why Article 4 DA is not simply entitled "access right" but "rights and obligations of users and data holders with regard to access". The issue of transferability is further analyzed at 3.

The right is non-waivable "to the detriment of the user", Article 7(2) DA, Article 8(2) DA. This seems to follow the scholarly proposal of a non-waivable access right.[21] By allowing contracts which are not to the detriment of the user, arguably, the door is open for contractual agreements "selling" the user right back to the data holder (by waiving the right against remuneration in the contract between the data holder and the user), but not for free. In other words, although uncompensated buy-out agreements will not be possible, a functioning data market that includes data holders on the demand side is feasible.

II. Exclusivity

The mechanism of Article 4(13)(14) DA and Article 8(4) DA, allocating the right of use and transfer within the relationship between data holder and user to the user, was already examined (see at II.3). In addition, and this is important to stress, trade secret protection steps in. To the extent trade secret protection for raw data is accepted, this protection not only acts for data holders but also for users (and recipients) as soon as they are in control of the data. The user enjoys trade secret protection against the recipient and other third parties. Because both the data holder and the user (and even the data recipient) are persons lawfully controlling the trade secret, both (or all) are trade secret holders in the sense of Article 2(2) TSD. The preservation of trade secrecy described at section II.2

---

[20] *Zech*, Data as a tradeable commodity, in: De Franceschi (ed.), New Features of European Contract Law – Towards a Digital Single Market, 2016, p. 51 (56).

[21] *Drexl*, Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation BEUC, 2018, p. 156-157.

not only serves to protect the data holders but, as an automatic effect, also the user, the data recipients, and further recipients. Trade secrecy therefore serves as a kind of tradeable IP right in the Data Act. It must be borne in mind however that trade secrets licenses are not genuine licensing agreements but only agreements to disclose trade secrets to the contracting party which in turn must keep it secret. This means that "licensing" trade secrets still causes higher transaction costs than licensing IP rights.

The preservation of trade secrecy is also reflected in Article 4(14) DA where the second sentence reads: "Where relevant, data holders shall contractually bind third parties not to further share data received from them." The obligation to prevent disclosure by third parties serves the user by upholding trade secrecy. This argument is reinforced by Recital 37 DA: "In order to prevent the exploitation of users, third parties to whom data has been made available at the request of the user should process those data only for the purposes agreed with the user and share them with another third party only with the agreement of the user to such data sharing." In effect, the Data Act envisages a chain of contracts binding recipients and further recipients and thereby upholding trade secrets protection.

III. Transfer

The key question when analysing the user's position is whether the user has a right to transfer (allowing the trading of his or her right). The answer to this question is clearly affirmative. Arguably, it is the key idea of the Data Act that the user may transfer (and trade) the data to whoever he or she likes. Recital 25 DA states: "This Regulation does not prevent users, in the case of business-to-business relations, from making data available to third parties or data holders under any lawful contractual term, including by agreeing to limit or restrict further sharing of such data, or from being compensated proportionately, for example in exchange for waiving their right to use or share such data." At least in business-to-business relations the user may transfer the data (or enable the transfer of the data)

(1) to holders, cf. Article 7(2), 8(2) DA, but not "to the detriment of the user" (see at III.1);
(2) to third parties (data recipients);
(3) to further third parties (further recipients), cf. Recital 33: "Upon the agreement with the user, and subject to the provisions of this Regulation, third

parties should be able to transfer the data access rights granted by the user to other third parties, including in exchange for compensation." Moreover, according to Recital 33 "data intermediaries ... may support users or third parties", clarifying that data intermediaries may trade the rights to further recipients.

The "data access rights granted by the user" mentioned in Recital 33 refers to the right of the user in Article 5 DA. When the user does not exert the right him- or herself but transfers the right to the data recipient (number 2 of the above-mentioned alternatives), a transferable right arises. The position of the data recipient may then be interpreted as "a party acting on behalf of a user" in the sense of Article 5(1) DA. The data recipient then is the "third party" according to Recital 33 transferring the data access rights to "other third parties". The wording of Recital 33 also allows for further transfers. All this, however, is only possible "[u]pon the agreement with the user".

To sum the position of the user up: The user enjoys exclusion not only against the data holder but also against third parties, by virtue of trade secret protection. The user enjoys a right to use, enabled by a right to access. Finally, the position is transferable, or, in the words of property rights theory, the user also enjoys a right to transfer. In essence, the position of the user fulfils all the criteria that constitute the core of property (see at I.1).

D. Co-ownership?

The question remains whether in the Data Act also aspects of co-ownership can be found. Property rights theory, in that respect, may serve as an analytical framework for managing shared assets. Co-ownership is distinct from a mere overlap of property rights. It entails a certain degree of joint management of an asset. As an example, §§ 741-758 BGB (German Civil Code) and similar rules in IP law may serve. For data, the ALI-ELI Principles for a Data Economy developed principles for co-generated data (Principles 18-23).[22]

---

[22] ALI/ELI Principles for a Data Economy, Data Transactions and Data Rights, As Adopted and Promulgated by The American Law Institute on May 18, 2021 and The European Law Institute on September 1, 2021 (Principles 18-23). Similar *Metzger/Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42 (55).

The Data Act arguably does contain some elements of co-ownership. The user profits from exclusivity derived from the data holder's trade secret protection. Both enjoy trade secrecy protection which they must uphold jointly. For a detailed analysis, different aspects of co-ownership may be discerned which can be derived from the "standard models" for co-ownership like co-ownership in tangible assets and in IP. This not only allows to clearly flesh out the effects of the Data Act data sharing mechanism but also to design appropriate contracts and model contracts.

As the core aspects of co-ownership may be mentioned:

(1) Use (both parties should have a use right), cf. § 743(2) BGB: Each party has a right to use as far as the other party's use is not afflicted. Here, the non-rivalrous nature of data use can be taken into account.

(2) Exclusion (against third parties, in that respect, co-ownership is different from open data).

(3) Transfer (including dereliction of the right, which for trade secrets would be the public disclosure of the secret).

Among further aspects of co-ownership may be mentioned (as a non-exhaustive list):

(4) Integrity, meaning the preservation of the asset.

(5) Management which, as the norm, is joint management (but can contractually be stipulated otherwise), cf. § 744(1) BGB, and includes safeguarding of the right.

(6) Fruits, meaning the distribution of gains derived from the management of the asset. For example, § 743(1) BGB distributes fruits corresponding to the share in co-ownership. Arguably, this is also the idea of the Data Act, cf. Article 9(1) and Recital 47: „may (also) include a margin". The data holder,

therefore, should also be entitled to a participation in economic gains, corresponding to his or her merit in generating the data.

E. Final assessment: Data access right(s) as an enabler for data markets and further fields of action

Finally, coming back to the main function of property rights, it may be asked whether the Data Act data sharing mechanism has the potential to enable data markets (cf. Recital 4: "a well-functioning internal market for data"). Regarding the transferable "data access rights" mentioned in Recital 33, this can clearly be answered in the affirmative. The position of the user as a whole is designed in a way to allow trading the resulting access rights to all interested parties, including the data holder him- or herself. This, hopefully, will lead to data markets fostering the use of raw data.

As a legal policy perspective, it is worth mentioning that the aim of arriving at functioning data markets can be helped by acting in two important areas of activity which are also mentioned in the Data Act and which do not require legislative action. The first is supporting data intermediaries (cf. Recital 26, 33) and personal information systems (PIMs). The second is the development of model contracts between data holders and users (cf. Article 41: "non-binding model contractual terms on data access and use") which may even include partnership contracts.

With model contracts, not only the optimum allocation of data but also distributional justice can be addressed (which is also underlying the non-waivability "to the detriment of the user", cf. section III.1). The idea should be to incentivize a co-operative utilization of raw data instead of an adversarial approach. The main function of the Data Act remains the enablement of functioning markets for raw data. The creation of a transferable access right seems to be a step in the right direction. With the development of proper model contractual terms (hopefully fostering co-operative acting on the markets), it might be even helped further.

Chapter 5

Contracts under the Data Act: Review of standard terms and FRAND conditions

Axel Metzger*

A. Introduction

Data access under the Data Act is provided as a non-contractual right. Requests under Article 4 do not presuppose a contract between the data holder and the product user. Still, data access requests will oftentimes (if not typically) occur between parties which have previously concluded a contract. Also, the parties may specify the details of data access requests in a contract after such a request is submitted to the data holder. The Data Act addresses the different contracts between the various parties involved, i.e. the product user, the distributor of the product, the data holder and possible third parties under Article 5 Data Act, most visible in Articles 13, 8 and 9, but also in the basic provisions of Articles 4 and 5. This chapter provides a critical analysis of the basic concepts underlying those provisions.

---

* Prof. Dr. Axel Metzger, LL.M. (Harvard), Chair of Private Law and Intellectual Property Law, Humboldt-Universität zu Berlin, Germany. This chapter is based on older works, see *Schweitzer/Metzger/Blind/Richter/Niebel/Gutmann*, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Study for the Federal Ministry for Economic Affairs and Climate Action, 2022, available at pure.mpg.de/rest/items/item_3457829_2/component/file_3457831/content (4.28.2024) and *Metzger/Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42.

B. Between market failure and market design

The contract law provisions of the Data Act are of a mandatory nature. Their aim is to provide the courts with the means to revise and correct contracts or individual provisions. This raises the question as to what kind of market failure the legislator is addressing with the rules. Unfortunately, the conceptual approach of the Data Act is not very clear. The recitals and the explanatory memorandum combine different goals: competition in aftermarkets, fairness for co-generators and consumer protection.[1] But none of the goals as such is justified by a sufficient economic analysis backed up with a coherent theory approach and empirical data. The overall impression is that the legislature is motivated by the very general goal of "unlocking the value of data in the EU" which rather appears as a market design approach instead of a clear market failure analysis. Still, even if one accepts that the allocation of use and access rights may be justified with the underuse of co-generated data (i.e. market design), any further intervention, especially a review of contracts, can only be justified if a clear market failure has been established with regard to the specific contractual situation.[2]

C. Role of contracts in the implementation of data access under the Data Act

Contracts may be concluded between the distributor of the product, the data holder, the product user and third parties. The Data Act addresses these contracts in different provisions which are discussed here in the order of a possible chronology of contacts between the parties.

---

[1] Regulation (EU) 2023/2854 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 2023/2854, 22.12.2023, p. 1-71, Rec. 5, 6.

[2] For a more detailed discussion of this approach see *Schweitzer/Metzger/Blind/Richter/Niebel/Gutmann*, Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, Study for the Federal Ministry for Economic Affairs and Climate Action, 2022, p. 70–115, available at pure.mpg.de/rest/items/item_3457829_2/component/file_3457831/content (28.4.2024).

I. Contract between user and distributor of the product

The first contract to be taken into account is the contract between the user and the distributor of the product which collects data. The distributor must not be the later data holder, e.g. if the farmer purchases a land machine from an agricultural machinery dealer. Still, the later data holder, e.g. the land machine producer, may impose terms on data access along the distribution chain.

Article 3(2),(3) provides for an information duty regarding the data generated by the product or related service. Before concluding a contract for the purchase, rent or lease of a product or the provision of a related service, clear and sufficient information should be provided to the (future) product user on how the data generated may be accessed. This obligation does not affect the obligation for the controller to provide information to the data subject pursuant to Articles 12, 13 and 14 GDPR.[3] A comparable information duty – with a different field of application – has already been enacted in Article 9(1) and (2) P2B Regulation,[4] according to which "online intermediation services" shall include in their terms and conditions a description of any personal data or other data which business users or consumers provide for the use of services concerned and of the technical and contractual access to such data.

Information duties of this kind, especially Article 3(2),(3), are of major importance for the effectiveness of the envisaged access rights.[5] (Potential) product users typically do not know what data is collected by the manufacturer or other data holders. This may prevent them from requesting access to data. The absence of information on what kind of data is available may be one of the reasons why data access requests have remained relatively rare so far. If the seller (or renter or lessor) fails to provide the information but still concludes a contract, such failure may either be qualified as non-conformity of the product, see Article 7(1)(d) Sales of Goods Directive or Article 8(1)(b) Digital Content Directive,

---

[3] Rec. 24 DA.

[4] Regulation (EU) 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, p. 57-79.

[5] Sceptical *Hennemann/Steinrötter*, Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW 2022, 1481 (1483), ("information overload").

or as misrepresentation during contract negotiations, depending on the applicable contract law principles. In addition, competitors may raise claims based on unfair competition law principles, at least in Germany.[6]

II. Contracts between product user and data holder

The Data Act is based on the premise that data holder and product user conclude a contract or even several different contracts.[7] A first contract between data holder and product user is presupposed in Article 4(13) for any use of the data *by the data holder*. This regime has been criticized during the legislative process since it creates a hold-up position for users reaching far beyond what is necessary to protect their legitimate interests.[8] The legislature has nevertheless implemented the rule. It is remarkable that the Data Act hardly foresees any mandatory or default rules for this contract, with the exception of Article 4(13), second sentence (and possibly Article 13), but leaves its design entirely to the parties' contractual freedom and national contract law.[9] Obviously, the European Commission did not see indications for a market failure here.[10]

In the framework of the same contract or in a second contract, the parties may specify the details of data access and the following use of the data *by the product user*. This contract may be concluded in the context of the sales, rental or lease agreement of the product or at a later stage, before or after a request based on Article 4 has been submitted to the data holder. The parties should have an interest to come to such an agreement, given the many difficult technical aspects of data access, starting with the exact scope and format of the data concerned and the time of delivery or access and extending to possible safeguards to

---

[6] § 3a UWG. Article 3(1), (2) DA should be considered as a "Marktverhaltensregel" and as such thus be eligible as a basis for competition law claims.

[7] *Staudenmayer*, Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz: Auf dem Weg zum Privatrecht der Datenwirtschaft, EuZW 2022, 596 (597).

[8] For a critique see *Bomhard/Merkle*, Der Entwurf eines EU Data Acts – neue Spielregeln für die Data Economy, RDi 2022, 168 (175); *Hennemann/Steinrötter*, Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW 2022, 1481 (1483); *Metzger/Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42 (54).

[9] *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 92 f. (Study Requested by the JURI committee).

[10] Critical for B2C contracts *Hennemann/Steinrötter*, Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW 2022, 1481 (1483).

keep the data secret etc. However, even though there may be good reasons to come to an agreement, the product user should not be obliged to enter into such a contract. The access right of Article 4 is a non-contractual right by nature. The product user has the right to go to court or lodge a complaint with the public authority under Article 38 even without a contract. It would then be up to the court to define the details of the product user's access to data, a task that courts will handle in parallel to the FRAND requirement of Article 8(1).[11] This puts the product user in a strong bargaining position for the negotiation of a contract. The data holder needs to conclude a contract in accordance with Article 4(13) and has an interest in fixing the details of the data access under Article 4. By contrast, the product user has all options at his or her disposal.

In light of the strong bargaining position of the product user, it seems appropriate to rely on the principle of freedom of contract with regard to these contracts. Still, there may be arguments to review standard clauses unilaterally imposed by the data holder. End users of products, e.g. consumers buying IoT devices or farmers leasing land machines, will typically not put much weight on the modalities of a later possible access to machine data. If the modalities of data access are not appreciated on the market as a valuable feature of the product, competitors may not compete over them ("lemon market").[12] In this regard, a review of standard terms may be justified as suggested by Article 13. By contrast, for major machine users, e.g. airlines, one can expect that the machine data collected is of sufficient commercial relevance.[13] Businesses should be in a position

---

[11] See *Picht,* Max Planck Institute for Innovation and Competition Research Paper No 22–12, 2022, p. 27–29, available at https://ssrn.com/abstract=4076842 (28.4.2024).

[12] On the justification of a review of standard terms based on the "lemon markets" problem see *Basedow,* in: Münchener Kommentar BGB, 9th ed. 2019, Vor § 305 BGB paras. 4–8.

[13] But see *Drexl* et al., 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), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, para. 125, available at https://ssrn.com/abstract=4136484 (7.4.2022), which pleads for a review of standard terms in case of non-SME users.

to consider the relevant clauses on data access carefully or take the risk of unfavourable conditions.[14] A review of standard terms is not appropriate in this case (but is nevertheless possible under Article 13).

The review of standard terms under Article 13 is of general application; it is not restricted to situations where a product user can claim data access according to the provisions of Article 4 but will also apply if the parties conclude a contract on a voluntary basis. The provision combines a blanket clause in Article 13(3) ("grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing") with a black and a grey list of unfair terms. For the terms of the blacklist in Article 13(4), e.g. on contractual limits of the liability of the party that unilaterally imposed the term or the remedies of the other party in case of non-performance or breach of contract, the Unfair Terms Directive 93/13[15] has apparently served as a blueprint. The provisions on the grey list in Article 13(5)(a),(g) again take up concepts from the Unfair Terms Directive but also provide for more specific standards of review for data access contracts in (b),(c), and (e), e.g. the presumption in (b) that a term is unfair that "allows the party that unilaterally imposed the term to access and use the data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party". Given the specific situation of users of data-generating products, it seems appropriate to review standard terms related to the access and use of data. However, it is questionable whether Article 13 should be used as a door opener to introduce a review of B2B standard contract terms of a general nature like terms on remedies and liability.[16]

---

[14] One way out of the review of standard terms is to negotiate the conditions individually which means that they fall out of the category of unilaterally imposed terms. Whether the legislature also wanted to exempt terms that are "simply provided by one party and accepted by the other enterprise", see Rec. 59, remains to be discussed. This would limit the scope of application of Article 13 significantly. See *Hennemann*, in: Lohsse/Schulze/Staudenmayer (eds.), Private Law and the Data Act, Münster Colloquia on EU Law and the Digital Economy VIII, 2024, Chapter IV (to be published).

[15] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34; *Staudenmayer*, Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz: Auf dem Weg zum Privatrecht der Datenwirtschaft, EuZW 2022, 596 (598) also points to the finally failed Common European Sales Law (CESL).

[16] See also *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, p. 107–109 (Study Requested by the JURI committee).

III. Contracts with third parties based on Article 5

1. Contract between data holder and third party

Finally, the data holder may enter into an agreement with a potential third party who is using the data based on the product user's request. As in the relationship between the data holder and the product user, Article 5 does not oblige the third party to enter into an agreement with the data holder. Access to data may be grounded on the product user's simple request under Article 4. Still, it will again often be in the best interest of the data holder and the third party to specify the details of data access, namely the exact scope and format of the data concerned, the time of delivery or access, safeguards to keep the data secret etc.

For those agreements, the Data Act seems to provide two legal means for courts to intervene. However, at closer scrutiny, none of the two seems appropriate if taken as an instrument to review a contract freely negotiated between the data holder and the third party.

According to Article 8(1), the data holder shall provide access under FRAND conditions. Given the fact that the data holder is the only entity that can grant access to the specific product user's data in question, it seems necessary to protect the third party from unfair or discriminatory access conditions. Without such a requirement, the data holder could dictate the terms of access to a third party. Nonetheless, the FRAND requirements of Article 8(1) should not be read to allow courts to review the conditions of a contract that has been concluded by the parties (see below, D.V.).

Still, the standard terms used in a contract between the data holder and the third party are subject to review in accordance with Article 13. However, it is questionable whether such a review is justified. For the third party, the access right will be of central interest. There is, therefore, no reason to expect a "lemon market" problem as described above. Imbalanced access terms will not result from the phenomenon that standard clauses are normally not read by SME parties – which would justify a review under Article 13. Rather, they may follow from a data holder's abuse of his or her monopoly position over the relevant user's data.[17] To address this problem, the FRAND mechanism in Article 8(1) is better suited.

---

[17] But see *Picht*, Caught in the Acts: Framing Mandatory Data Access Transactions Under the Data Act, Further EU Digital Regulation Acts, and Competition Law, Max Planck Institute

2. Contract between product user and third party

Regarding the relationship between users and third parties, Article 6(1) seems to presuppose that the parties conclude a contract under which the third party may use the data ("under the conditions agreed with the user"). The conclusion of such a contract is not a necessary precondition for the use of the data by a third party, but its conclusion is indeed likely. Unfortunately, the Data Act does not clarify whether the third party may pay money as consideration for the user's willingness to make a request. In the prototypical situation, a product user will empower a third party to act on his or her behalf because he or she is interested in the third party's complementary service. But there may be situations where this motivation is not sufficient – e.g. because the third party's service is still in an early stage of its development. At least when it comes to non-personal data, a decision of a product user to "monetize" his or her data in such a way should be accepted if the legislature wants to reach its goal of opening new opportunities for aftermarket services.

IV. Lack of model contract terms or default rules

The analysis so far has addressed mandatory provisions for contracts between data holders, product users and third parties. For the well-functioning of markets, it will be equally important to develop model contract terms which the parties may apply as blueprints for their contracts or, at least, as a starting point for their negotiations. Once the market has developed business practices, those practices may be further developed into (majoritarian) default rules to be applied by courts in case of incomplete contracts. Up to now, neither model terms nor default rules suitable for the implementation of mandatory access rights are sufficiently developed.

The Data Act addresses the issue of a lack of model terms or defaults. According to Article 41, it is on the European Commission to "develop and recommend non-binding model contractual terms on data access and use". The development of such terms will not be trivial and will take some time given that markets are just emerging.

---

for Innovation and Competition Research Paper No 22–12, 2022, p. 38 ff., available at https://ssrn.com/abstract=4076842 (28.4.2024).

The most advanced soft-law instrument for data access contracts already available are the "ALI-ELI Principles for a Data Economy".[18] The Principles are not specifically tailored to data access contracts based on mandatory access rights. Still, they may be useful as a source of inspiration. Principle 20 ("Access or porting with regard to co-generated data") provides a list of circumstances of a possible legitimate use of co-generated data. Principle 21 ("Desistance from data activities with regard to co-generated data") describes possible restrictions in the use of such data based on the legitimate interests of the data holder. The circumstances listed may be the basis for defaults in data access contracts since they describe what the co-generator may expect. Principle 7 ("Contracts for the transfer of data") and Principle 8 ("Contracts for simple access to data") provide sets of contract law principles for data transfer or data access contracts. Even though drafted for voluntary data contracts, these principles may still be useful for a further specification of data access agreements concluded on the basis of Article 4 or Article 5.

D. Access to data under FRAND conditions

According to Article 8(1), a data holder, where obliged to make data available to a data recipient under Article 5 or "under other applicable Union law or national legislation adopted in accordance with Union law," shall do so "under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner". Given the broad language, Article 8 may have an impact also for access rights based on the DMA – but not on competition law in a strict sense, see Recital 116. The so-called FRAND requirement is not novel to EU market regulation. It has been referred to in competition cases where a refusal to license intellectual property rights was found to constitute an abuse of dominance under Article 102 TFEU, and it has been applied to copyright in databases[19] and software.[20] Standard-setting organisations (SSOs) require their members to

---

[18] ALI-ELI Principles for a Data Economy, Data Transactions and Data Rights, As Adopted and Promulgated by The American Law Institute on May 18, 2021 and The European Law Institute on September 1, 2021, 2023.

[19] CJEU, Judgement of 29.4.2004, IMS Health, C-418/01, ECLI:EU:C:2004:257.

[20] CJEU (General Court), Judgement of 17.9.2007, Microsoft v Commission, T-201/04, ECLI:EU:T:2007:289.

commit to license standard essential patents (SEPs) on FRAND terms, and undertakings who have accepted a FRAND commitment are obliged to engage in "good faith" negotiations with potential licensees before suing for injunctions.[21] A simplified FRAND test is also applied in sector-specific regulations.[22] Even though Article 8 is apparently drafted against this backdrop, experience from the older FRAND licensing schemes should only be used with some caution.

I. Addressees of the FRAND requirement

Article 8 seems to suggest that, within the framework of the Data Act, only third parties that are granted data access under Article 5 should benefit from the FRAND requirement. However, such an interpretation would draw the circle of eligible addressees too narrow. If product users request data access under Article 4, courts will have to define the terms of such access as well. According to Article 4(1), access to data has to "be free of charge". But free of charge does not mean that the data holder may push through access conditions of an unfair, unreasonable or discriminatory nature.[23] The proviso "or under other applicable Union law" may serve as basis for including product users into the FRAND regime of Article 8, even though it is admitted that this would require an extension of the provision *praeter legem*.

II. What data is licensed under FRAND requirements?

Licensing of SEPs on FRAND terms may appear to be straightforward with regard to the licensed subject matter, which is a clearly defined registered right. However, the practical experience turned out to be different and raised complicated issues since patent holders, when asked for a non-discriminatory patent

---

[21] CJEU, Judgement of 16.7.2015, Huawei Technologies, C-170/13, ECLI:EU:C:2015:477.

[22] See e.g. Article 61 Regulation (EU) 2018/858 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, 14.6.2018, p. 1-218.

[23] *Picht*, Caught in the Acts: Framing Mandatory Data Access Transactions Under the Data Act, Further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No 22–12, 2022, p. 27–28, available at https://ssrn.com/abstract=4076842 (28.4.2024).

license, replied that they would only be willing to grant licenses for a given patent portfolio and on a worldwide basis whereas the potential licensees would only ask for a license for a specific patent for a specific state or region and therefore ask for a lower license fee.[24] Questions of this kind should not come up with regard to data accessed on the basis of a specific user request under Article 5. Still, there may be issues with regard to the specific structure and format of the data and the technical means of access. These technical requirements should be specified in accordance with the technical requirements mentioned in (and further developed in practice under) Article 4(1).

III. Who determines FRAND requirements?

The question of who should determine FRAND requirements and in what procedural setting is the subject of a broad debate with regard to SEPs. Yet, not all of the issues discussed with regard to SEPs are topical when it comes to data access. Potential licensees of SEPs are typically not depending on the patent holder's technical cooperation for the use of the protected standard. Usually, they know the technology from the SSO or from elsewhere and are merely in need of a license to use it. Therefore, in a typical procedural setting, it is not the potential licensee but the patent holder who initiates proceedings and sues the potential licensee for patent infringement.[25] The patent holder's obligation to grant a FRAND license for the use of the SEP will then be brought forward as a defense. Actions of potential licensees with the aim to force holders of SEPs into FRAND license agreements have not been reported so far, at least in Germany.[26]

Court proceedings on data access claims under Article 4 or 5 will likely follow a different pattern. In this setting, the user or the third party depends on the data holder's technical cooperation to get access to the data in question. Therefore, the product user or third party will typically be on the claimant's side of a court

---

[24] See for the discussion of this issue *Hauck/Kamlah*, Was ist „FRAND"? Inhaltliche Fragen zu kartellrechtlichen Zwangslizenzen nach *Huawei/ZTE*, GRUR Int. 2016, 420 (423–425).

[25] *Drexl* et al., 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), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, para. 102, available at https://ssrn.com/abstract=4136484 (7.4.2022).

[26] *Walz/Benz/Pichelmaier*, Obligatorische Schlichtung bei FRAND-Streitigkeiten (Teil 1), GRUR 2022, 446 (447).

case and the data holder on the defendant's bench. Such a scenario, though different from the typical SEP case, is not new in the case law on Article 102 TFEU. It resembles the setting in the *Microsoft* case where the General Court confirmed a decision by the European Commission which obliged Microsoft to make interoperability information available to other undertakings having an interest in developing and distributing workgroup server products and to provide such information on the basis of FRAND terms.[27] A similar setting could arise if, as provided for in Article 37, public authorities of Member States would enforce the access rights of Articles 4 and 5 and the data holder would then lodge a complaint at the competent courts. In addition, users or third parties could bring suits before the regular courts which would then have to decide directly on the existence of an access right and on the applicable FRAND conditions under which the data holder would have to grant access. It can be expected that both the data holder and the product user or third party will suggest such conditions in their pleadings. It would then be up to the public authority or court to decide which of the suggested terms complies with the requirements of the FRAND test.

Commentators have criticized the handling of SEP patent license cases by regular courts. Courts may indeed not be best suited to establish appropriate contract terms.[28] Also, one may have doubts whether an infringement procedure on a specific patent allows the court and the parties to come to a decision on FRAND terms for broader international patent portfolios.[29] Therefore, it has been suggested to advise parties to refer their disputes to arbitration[30] or to prescribe a mandatory dispute settlement procedure before the parties can bring

---

[27] CJEU (General Court), Judgement of 17.9.2007, Microsoft v Commission, T-201/04, ECLI:EU:T:2007:289, para. 48.

[28] See from the abundant literature *Picht*, Schiedsverfahren in SEP/FRAND-Streitigkeiten, GRUR 2019, 11; *Schaefer/Czychowski*, Wer bestimmt, was FRAND ist?, GRUR 2018, 582; *Walz/Benz/Pichelmaier*, Obligatorische Schlichtung bei FRAND-Streitigkeiten (Teil 1), GRUR 2022, 446 (448).

[29] *Hauck/Kamlah*, Was ist „FRAND"? Inhaltliche Fragen zu kartellrechtlichen Zwangslizenzen nach *Huawei/ZTE*, GRUR Int. 2016, 420 (423–425).

[30] *Picht*, Schiedsverfahren in SEP/FRAND-Streitigkeiten, GRUR 2019, 11; *Schaefer/Czychowski*, Wer bestimmt, was FRAND ist?, GRUR 2018, 582 (584 f.).

their case before a court.[31] It may indeed be assumed that such alternative dispute resolution bodies may be better equipped to gear the parties into constructive contract negotiations. They are not bound by the tight corset of civil procedural rules, may be chosen by the parties and may therefore have special expertise in the area. Article 10(1) takes up these ideas and provides that data holders and data recipients shall have access to certified dispute settlement bodies. However, such a settlement procedure does not affect the right of the parties to seek an effective remedy before a court or tribunal of a Member State, see Article 10(13).

IV. Royalties

The Proposal for the Data Act did not offer any guidance as to how royalties for FRAND licenses based on Article 8(1) should be determined. Article 9(1), (2) and (3) in its final version has now implemented a primarily cost-based approach which restricts the data holder to calculate the compensation based on the costs incurred in making the data available, the investments in the collection and production of data and based on the volume, format and nature of the data. The data holder's compensation may also include a margin, see Article 9(1). However, according to Article 9(4), where the data recipient is an SME or a not-for-profit research organisation, any compensation agreed shall not exceed the costs referred to in Article 9(2), point (a). Moreover, the data holder must provide the recipient with information setting out the basis for the calculation of the compensation, Article 9(7). In addition to these rather rigid rules, the Commission shall adopt guidelines on the calculation of reasonable compensation, Article 9(5).

V. Relationship of FRAND requirements and review of (standard) contract terms

What remains to be clarified is the relationship of a contract concluded between the data holder and the third party and the FRAND requirements of Article 8(1). The FRAND requirements of Article 8(1) are designed as a yardstick for public authorities, courts or dispute settlement bodies which have to decide on

---

[31] *Walz/Benz/Pichelmaier*, Obligatorische Schlichtung bei FRAND-Streitigkeiten (Teil 1), GRUR 2022, 446 (513).

a claim for access.[32] They are not meant as a standard of review for contracts concluded between the parties.[33] One should not allow the third party to set aside a contract with the argument that its terms are not fair and reasonable or that they discriminate between third parties. Otherwise, this would result in a review that would apply to both standard terms and individually negotiated contracts and as such be more far-reaching than the review foreseen under Article 13. It should be borne in mind that the third party is under no obligation to conclude a contract with the data holder. Also, the European Commission has not presented any evidence for a systemic structural imbalance of power or other market failure between data holders and third parties that would justify such a far-reaching review across the board. Rather, it seems appropriate to leave the parties with the two possible, but independent ways to specify the conditions of data access: Firstly, the parties can come to an agreement "under the shadow" of Article 8(1) – i.e. the third party may use Article 8(1) as a bargaining chip. The agreement may also be reached as part of a settlement in proceedings. Such contracts should then be respected and not reviewed. Secondly, the parties may not agree on a contract. In this case, the third party may initiate proceedings before public authorities, courts or dispute settlement bodies and apply for access on FRAND terms. Admittedly, a third party who wants to offer services for which it depends on user data may be under pressure to rather conclude an unfavourable contract than wait for a public authority or court to issue a FRAND decision. But in this regard, procedural means, like preliminary measures, are the tool of choice to protect the third party. A generalized substantive review of contracts between businesses, including individually negotiated terms, would be overly intrusive. If, on the other hand, an imbalance of power exists, due to a position of dominance of the data holder or a dependence of the third party on the data holder, competition law – including § 20(1a) GWB – remains applicable and would provide the substantive standard to be applied to the contractual

---

[32] See also *Drexl* et al., 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), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, para. 101, available at https://ssrn.com/abstract=4136484 (7.4.2022).

[33] This is also expressed in Rec. 42 DA: "Voluntary data sharing remains unaffected by those rules."

conditions. General civil law doctrines like ordre public or "gute Sitten", e.g. § 138 BGB, may be invoked as a last resort.

E. Conclusion

The basic approach of the Data Act is characterized by mistrust of the self-regulating forces of the market. Instead of offering default rules for data contracts, the legislator favors mandatory, non-contractual access rights and judicial control of the contracts based on these rights, at least when it comes to standard contracts. The legislature is thus defining the structure of the market for machine data. Whether this regulatory approach actually achieves the desired effects of market liberalization can be observed from September 2025.

Part III

Challenge 1: The Semantic Level of Data

Chapter 6

The Data Act and trade secrets: an experiment in compulsory licensing

Tanya Aplin*

A. Introduction

Compulsory licences are a feature of intellectual property law, most often associated with patents and copyright and, to a lesser extent, plant variety rights.[1] In essence, a compulsory licence may be described as a state sanctioned, non-exclusive permission to use subject matter protected by an IP right, without the authorisation of the rightholder, in order to serve the public interest and conditional upon reasonable remuneration. From a policy point of view, the effectiveness of compulsory licences for patented medicines has been fiercely debated[2] and the introduction of a compulsory licence mechanism to the EU sui generis database right has been suggested at various points.[3]

---

* Prof. Dr. Tanya Aplin, Professor of Intellectual Property Law at the Dickson Poon School of Law, King's College London, United Kingdom. She would like to thank Prof. Ulla-Maija Mylly for her helpful comments on a draft version of this chapter.

[1] See *Bonadio/Hingorani*, Compulsory Licensing of Intellectual Property, in: Sappa (ed.), Research Handbook on Intellectual Property Rights and Inclusivity, Edward Elgar 2024, p. 440.

[2] E.g. *Thambisetty* et al., Addressing Vaccine Inequity During the Covid 19 Pandemic: The TRIPs Intellectual Property Waiver Proposal and Beyond, 81(2) Cambridge Law Journal 384, 2022, discussing the drawbacks of compulsory licensing and arguing instead for an 'IP waiver'.

[3] *Leistner*, The existing European IP rights system and the data economy – an overview with particular focus on data access and portability, in: German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for

Innovation and Competition (eds.), Data access, consumer protection and public welfare, Nomos 2021, p. 209 (244).

Trade secrets protection in the European Union (EU) falls under the broad umbrella of intellectual property law,[4] albeit it is more accurately characterized as a type of unfair competition liability than as a property right.[5] Therefore, at first sight, it may seem strange to raise the issue of compulsory licensing of trade secrets. However, it is not surprising when one considers that, despite trade secrets protection not being a property right, there is regularly voluntary licensing of trade secrets.[6] Further, this very issue came to the fore during the Covid-19 pandemic, with the realization that compulsory licensing of patented vaccines was insufficient without access to the associated know-how about how best to manufacture them. This led to calls for extending compulsory licences to trade

---

[4] See Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), as signed 15 April 1994, as amended 6 December 2005, Art. 39; see also *Bently*, Trade Secrets: "Intellectual Property" But Not "Property"?, in: Howe/Griffiths (eds.), Concepts of Property in Intellectual Property Law, CUP 2013, p. 60.

[5] *Knaak/Kur/Hilty*, Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for a Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against their Unlawful Acquisition, Use and Disclosure of 28 November 2013, Com(2013) 813 Final, 45(8) IIC - International review of intellectual property and competition law 953, Max Planck Institute for Innovation & Competition Research Paper No. 14-11 (paras 16-17), 2014. Although note the suggestion that EU trade secrets law is a hybrid between intellectual property and unfair competition laws: see *Ohly*, Germany: the Trade Secrets Protection Act of 2019, in: Schovsbo/Minssen/Riis (eds.), The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive, Edward Elgar 2020, chapter 7; or, at the very least, shows conceptual ambivalence: *Aplin*, The Limits of EU Trade Secret Protection, in: Sandeen/Rademacher/Ohly (eds.), Research Handbook on Information Law and Governance, Edward Elgar, 2021, p. 174.

[6] *Hull*, The licensing of trade secrets and know-how, in: de Werra (ed.), Research Handbook on Intellectual Property Licensing, Edward Elgar 2013, p. 155. Hull explains that there are broadly two types of licence – the 'pure' trade secret/know-how licence and the technical assistance/know-how licence.

secrets during public health emergencies and its justification under TRIPS.[7] We see this type of proposal being taken forward in the EU, for example.[8]

Against this background, what is the relevance of the European Union's recently adopted Data Act[9]? The answer is that it provides us with a concrete example of compulsory licensing of trade secrets in the sphere of IoT data. As such, there may be lessons to be drawn from this experiment when thinking about the nature of compulsory licenses for trade secrets in other contexts. This chapter will analyse the provisions of the Data Act which interface with trade secrets[10] and, by comparing these with the features of compulsory licences for IPRs, discuss how the Data Act arguably creates a compulsory licence for trade secrets.[11]

B. Subject matter of the compulsory licence

Compulsory licences for IPRs usually have a clear subject matter. They may relate, for example, to a patented invention, a copyright work, or a related right, such as a plant variety right.[12] They are precluded, however, for registered trade

---

[7] See *Levine/Sarnoff*, Compelling Trade Secret Sharing, 74 Hastings LJ 987, 2023; *Gurgula/Hull*, Compulsory licensing of trade secrets: ensuring access to COVID-19 vaccines via involuntary technology transfer, 16 *Journal of Intellectual Property Law & Practice* 1242, 2021, https://doi.org/10.1093/jiplp/jpab129; *Gurgula/McDonagh*, Access Denied: the Role of Trade Secrets in Preventing Global Equitable Access to COVID-19 Tools, March 2023, StopAids & JustTreatment, available at https://ssrn.com/abstract=4484507 (19.6.2024).

[8] Discussed by *Gurgula*, On the European Commission's proposal to create a new EU-wide compulsory licensing regime, 46 European Intellectual Property Review 70, 2024.

[9] 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 2023/2854, 22.12.2023, p. 1-71.

[10] See also *Zech*, Data Access Rights as Property Rights (Chapter 4 in this volume).

[11] As first identified by *Drexl* et al., 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), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, doi.org/10.2139/ssrn.4136484, para. 286.

[12] See Art. 31 TRIPS; Berne Convention for the Protection of Literary and Artistic Works (Berne), as signed 9 September 1886, as amended 28 September 1979, Art. 13 (musical works) and Art. 21 and Appendix; Universal Copyright Convention (UCC), as signed 6 September 1952, as revised 24 July 1971, Arts. Vter and Vquater; and Council Regulation (EC) No

marks.[13] The subject matter is identifiable in the case of registered IPRs, such as patents and plant variety rights, because the registration process forces the applicant/proprietor to articulate the invention (i.e. in the claims of the patent specification)[14] and to identify the technical details and origin of the plant variety, along with its botanical taxon and provisional designation.[15] In the case of unregistered rights, such as copyright, the fixation of the work can help to define its boundaries.[16]

When it comes to identifying trade secrets there are some inherent difficulties. The first is that the legal definition of 'trade secret' is broad and flexible: it envisages the subject matter as secret information which has commercial value due to its secrecy and for which reasonable steps under the circumstances have been taken to maintain secrecy.[17] Apart from the issue of whether it is possible to confidently assess whether the requirements of secrecy, commercial value, and reasonable steps have been met, there is a second difficulty, which is that secret *information* may be diffuse. A person may claim that an expansive set of data constitutes a trade secret and the boundaries of this may be hard to identify. These are well-known, existing difficulties to which we have seen practical responses. In the case of voluntary trade secret licences, it will be typical to specify the trade secret by reference "to a specified document...a library of documents; a database; specifications; drawings, formulae and so on".[18] Moreover, when involved in trade secret litigation (at least in common law jurisdictions), judges have called for the trade secret to be specifically pleaded.[19]

In the Data Act, the compulsory licence relates to "product data" and "related service data" along with any relevant metadata, which *also* qualify as a *trade*

2100/94 of 27 July 1994 on Community plant variety rights (CPVR), OJ L 227, 1.9.1994, p. 1-30, Art. 29(1).

[13] Art. 21 TRIPS.

[14] Art. 29 TRIPS.

[15] Art. 50 CPVR.

[16] *Sherman*, What is a Copyright Work?, 12(1) Theoretical Inquiries in Law 99 (108), 2011.

[17] Art. 39 TRIPS; and Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (TSD), OJ L, 2016/157, 15.6.2016, p. 1-18, Art. 2(1).

[18] *Hull*, The licensing of trade secrets and know-how, in: de Werra (ed.), Research Handbook on Intellectual Property Licensing, Edward Elgar 2013, p. 155 (177).

[19] E.g. in England and Wales, *Ocular Sciences Ltd v Aspect Vision Care Ltd*, [1997] RPC 289, 360.

secret within Article 2 of the EU Trade Secrets Directive (TSD).[20] This somewhat circuitous identification is due to the Data Act's primary focus on sharing data from connected products; however, there is a recognition that such data may also qualify as a trade secret and that measures must be taken to preserve confidentiality whilst at the same time enabling access.[21] Therefore, the starting point is identifying "product data", "related service data" and "metadata", as defined in Article 2 of the Data Act:

(2) 'metadata' means a structured description of the contents or the use of data facilitating the discovery or use of that data;

(15) 'product data' means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer;

(16) 'related service data' means data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider;

Recital 15 of the Data Act refines which data fall within the scope of the legislation:

data which are not substantially modified, meaning data in raw form, also known as source or primary data which refer to data points that are automatically generated without any further form of processing, as well as data which have been pre-processed for the purpose of making them understandable and useable prior to subsequent processing and analysis...

Next, the question is whether raw data, pre-processed data, and metadata from connected products and related services constitute a *trade secret*. There is no reason to think such data would not qualify as *information* given that "data" is defined broadly as "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-recording".[22] However, it is not straightforward that such data will have the required commercial value due to secrecy.[23] Recital 14 of the TSD indicates that "value" may be assessed by the harm caused by trade secret

---

[20] Arts. 2, 4(1), 4(6), 5(1), 5(9), 15 and 20(3) Data Act.

[21] For an analysis of those data sharing rights as property rights see *Zech*, Data Access Rights as Property Rights (Chapter 4 in this volume).

[22] Art. 2(1) Data Act.

[23] As required by Art. 2(1)(b) TSD.

misappropriation, where harm is conceptualised broadly as undermining various interests – whether they be technical, business, financial, or the ability to compete. To put it in the positive sense, the question is whether the information provides a competitive advantage *because it is secret.* Meanwhile, information is considered "secret" if it is not "generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question".[24]

For raw, pre-processed and meta data to have commercial value these would need to be aggregated at some level.[25] Moreover, the data must be secret and there must be a causal link between any commercial value and the secrecy of the information. Whether these requirements are met will depend on the type of data generated by a connected device and attitudes of the manufacturer and user of connected devices to secrecy. [26] Also, the causal link is more likely to exist where a manufacturer of a connected device aggregates data from multiple devices in order to improve those devices or to be used in secondary markets (such as for AI training data).[27] It seems likely that industry will struggle reliably to identify whether raw, pre-processed and meta data satisfies the definition of "trade secret"; however, it is also likely that, despite the difficulty of an *ex ante* assessment, data holders will, as a matter of practicality, treat such data as trade

[24] Art. 2(1)(a) TSD.

[25] *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Nomos 2017, p. 59; and *Drexl*, Data Access and Control in the Era of Connected Devices, Study on behalf of BEUC, 2018, available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf (19.6.2024), p. 93-94.

[26] *Drexl*, Data Access and Control in the Era of Connected Devices, Study on behalf of BEUC, 2018, available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf (19.6.2024), p. 94 gives the example of a smart meter measuring the consumption of energy as one where there may be limited data and where the maker and user of the connected device have no real interest in secrecy.

[27] *Aplin*, Trading Data in the Digital Economy: Trade Secrets Perspective, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017; *Drexl*, Data Access and Control in the Era of Connected Devices, Study on behalf of BEUC, 2018, available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf (19.6.2024), p. 94.

secrets.[28] The fact that data holders are obliged to *identify* which data is protected as a trade secret will not necessarily change this practice.[29] However, the identification will serve the purpose of enabling users and third parties to know which data will require them to take proportionate technical and organizational measures to preserve confidentiality (discussed below in section E).

Finally, it is crucial to remember which data are *not* covered by the Data Act, such that, even if protected as a trade secret, these data would not be subject to a compulsory licence. Recital 15 of the Data Act clarifies that *processed data* are excluded and describes this as "information inferred or derived from [raw or pre-processed data], which is the outcome of additional investments into assigning values or insights from the data, in particular by means of proprietary, complex algorithms". It seems more likely for processed data to qualify as a trade secret because of the commercial value attached to it and, because of this value, the likelihood that it will be kept secret. Yet, the exclusion of processed data means that the Data Act creates a very narrow range of subject matter that is eligible for a compulsory licence of trade secrets. Indeed, commentators have criticized this exclusion of processed data as undermining the overall usefulness of the Data Act.[30]

C. Justification/s for the compulsory licence

Compulsory licences for IPRs are underpinned by public interest and the type of public interest at stake may vary, whether to promote cultural access and education, deal with health emergencies and other public health concerns, or rectify market failures. For example, both the Berne Convention (Berne) and Universal

---

[28] This is borne out by the empirical data: see *Aplin* et al., The role of EU trade secrets law in the data economy: an empirical analysis, 54 IIC 826 (835-836), 2023, https://doi.org/10.1007/s40319-023-01325-8.

[29] Arts. 4(6), 5(9) and 19(3) Data Act.

[30] *Drexl* et al., 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), (2022), Max Planck Institute for Innovation & Competition Research Paper No. 22–05, 2022, https://doi.org/10.2139/ssrn.4136484, paras 24-25; *Kerber*, Governance of IoT data: why the EU Data Act will not fulfil its objectives, 72 GRUR International 120 (126-127), 2023, https://doi.org/10.1093/grurint/ikac107.

Copyright Convention (UCC) contain compulsory licence provisions for developing countries, in relation to translation of copyright works for teaching, scholarship, or research purposes and reproduction of literary, scientific or artistic works for systematic instructional activities.[31] In the case of patents, Article 31 of TRIPS does not restrict the purpose of any compulsory licence, however, it does relax the condition of reasonable efforts to obtain a voluntary licence in cases of "national emergency or other circumstances of extreme urgency or in cases of public non-commercial use". Further, in Article 31*bis* of TRIPS the purpose is to enable countries without manufacturing capacity to import pharmaceutical products made pursuant to a compulsory licence from eligible exporting countries. At national level, we also see instances of compulsory licences for patents that are justified by failure to meet demand for patented products on reasonable terms or where a patent is being used in an economically harmful way.[32] In the case of plant variety rights, both health and market concerns are at play, given that the following purposes constitute a public interest that justifies a compulsory licence: "(a) the protection of life or health of humans, animals or plants; (b) the need to supply the market with material offering specific features; (c) the need to maintain the incentive for continued breeding of improved varieties."[33]

There are two distinct purposes served by compulsory licences of trade secrets within the Data Act.[34] The first is economic in nature, namely, to avoid market failure in the sharing of data and to promote competition.[35] The desire

---

[31] Appendix, Arts. I-III Berne; Arts. Vter and Vquater UCC. Discussed by *Ulmer*, The Revision of the Copyright Conventions in the Light of the Washington Recommendation, 1 IIC 235, 1970.

[32] E.g. s. 48A Patents Act 1977 (UK).

[33] See Commission Regulation (EC) No 874/2009 of 17 September 2009 establishing implementing rules for the application of Council Regulation (EC) No 2100/94 as regards proceedings before the Community Plant Variety Office, OJ L, 2009/251, 24.9.2009, p. 3-28.

[34] When this chapter describes compulsory licensing of *trade secrets* in the context of the Data Act, it is referring to eligible data within the scope of the Data Act that is *also* protectable as a trade secret, as discussed in Section B.

[35] For a discussion of the interplay between competition law and the Data Act see chapter 3 in this volume by Prof. Weck. Suggesting that the economic reason is market *design* rather than market *failure* see *Metzger*, Contracts under the Data Act: Review of standard terms and FRAND conditions (Chapter 5 in this volume).

is to combat the *de facto* ability of manufacturers of connected products to control what data are generated and accessible[36] and to "allow for the emergence of liquid, fair and efficient markets for non-personal data in the Union".[37] In turn, this will enable "users of connected products to benefit from aftermarket, ancillary and other [novel] services based on data collected by sensors embedded in such products".[38] This is the case even if an aftermarket service is in competition with a service provided by a data holder.[39] The second purpose is a public interest in allowing public sector bodies[40] to carry out their functions in cases of exceptional need. These are characterized as relating to public emergencies, such as those relating to health, natural disasters or major cybersecurity interests,[41] or where lack of data prevents the public sector body from fulfilling a specific task in the public interest.[42]

Unlike copyright and patents, where Berne/UCC and TRIPS, respectively, specify the purpose of the compulsory licence or deliberately leave the purpose open, there is nothing in TRIPS which expressly regulates compulsory licences of trade secrets. Commentators have suggested that TRIPS does not prohibit compulsory licensing of trade secrets because i) there is no express exclusion (as there is for trade marks); ii) the wording of Article 39 of TRIPS does not point in this direction; and iii) the drafting history also supports this view.[43] While these are persuasive arguments, there is still the question of which *purposes* would justify a compulsory licence of trade secrets. Commentators have argued that Article 73 of TRIPS would justify compelled sharing of trade secrets in cases of national emergency, such as a pandemic,[44] however, this does not address the situation where the purpose is to deal with market failure. In short, there is more scope for analysing whether TRIPS Members have complete discretion when it comes to compulsory licensing of trade secrets for different

---

[36] Rec. 20 Data Act.

[37] Rec. 26 Data Act.

[38] Rec. 16 Data Act. See also rec. 32.

[39] Rec. 30 Data Act.

[40] The provision refers to public sector body, the Commission, the European Central Bank or a Union body, however, "public sector bodies" is being used here to refer to these collectively.

[41] Art. 15(1)(a) and recs. 63 and 64 Data Act.

[42] Art. 15(1)(b) and rec. 65 Data Act.

[43] *Levine/Sarnoff*, Compelling Trade Secret Sharing, 74 Hastings LJ 987 (1019-1027), 2023.

[44] *Levine/Sarnoff*, Compelling Trade Secret Sharing, 74 Hastings LJ 987 (1027-1028), 2023.

purposes. However, we may take reassurance from the fact that compulsory licences of IPRs may be granted for a variety of public interests, including health and economic reasons, and so the Data Act is in keeping with existing practices.

D. Rights granted by the compulsory licence

Compulsory licences for IPRs specify which exclusive rights the licensee is entitled to undertake. For example, in the case of compulsory licences available to developing countries under Berne and the UCC, the licence permits the acts of translation or reproduction of a work and distribution of copies of that translation or reproduction within the country but does not permit the export of such copies.[45] In the case of patents, the scope and duration of rights granted by any compulsory licence "shall be limited to the purpose for which it was authorized" and shall be non-exclusive, generally non-assignable and for the supply of the domestic market.[46]

Articles 4(1) and 5(1) of the Data Act give users, or third parties as requested by a user, the right to *access* and *use* data and relevant metadata from their connected products or related services. This access must be "without undue delay" and the data must be "of the same quality as is available to the data holder, easily, securely, free of charge [to the user], in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time."[47] However, the user is precluded from using the data to develop a competing connected product and from sharing the data with a third party for this purpose.[48] These rights exist even if the data is also a trade secret although, as we will see in the next section, there are various conditions that must be met by users and third parties.

In the case of public sector bodies, there is a right to *access* and *use* certain data and relevant metadata in cases of exceptional need (as described above). Where

---

[45] Appendix, Arts. I-III Berne; Arts. Vter and Vquater UCC.

[46] Arts. 3(c)-(f) TRIPS.

[47] Arts. 4(1) and 5(1) Data Act.

[48] Art. 4(10) Data Act. Competing aftermarket services are, however, acceptable: rec. 30 Data Act.

this data is a trade secret, there is a right to access only to the extent necessary to address the case of exceptional need.[49]

The right to *access* and *use* data tracks the protection available under Article 4(1) of the TSD regarding unlawful *acquisition* and *use* of the trade secret. What is noticeably absent from this compulsory licence is the right of users, third parties or public sector bodies to *disclose* data that may be a trade secret. This is understandable because compulsory licences by their nature do not require the exercise of all exclusive rights and should not destroy the subject matter of the IPR. For trade secrets protection, it is crucial that information is *secret,* has commercial value *due to secrecy* and reasonable steps are taken *to preserve secrecy.* Granting a right to *disclose* the trade secret would be tantamount to destroying the subject matter of protection. Whereas, in the case of compulsory licenses for IPRs, such as patents and copyright, the same risk does not exist. If there is a compulsory licence to make and supply a patented product, this does not detract from the validity of the patent. Likewise, a compulsory licence to translate a copyright work in certain circumstances does not mean copyright no longer exists or that exclusive rights may not be exercised against other third parties. Thus, in the case of compulsory licences of trade secrets within the Data Act, it makes sense to restrict the rights to those of access and use and to exclude disclosure.[50] However, the *use* of data, if done carelessly or excessively, might threaten the continued secrecy of the information. As such, it is unsurprising that we see obligations placed on the licensee to ensure that secrecy of the data is preserved.[51] We turn now to discuss these obligations in more detail.

E. Obligations on the licensee

Articles 4(6) and 5(9) of the Data Act, in relation to users and third parties who access and use data, mandate that "trade secrets shall be preserved". This requires the data holder (or the trade secret holder if they are not the same person) to *identify* the data protected as trade secrets and to agree with the user/third party "proportionate technical and organizational measures necessary to preserve the confidentiality of the shared data". These measures include "model contractual

[49] Art. 19(3) Data Act.

[50] This probably explains Art. 11(2)(d) and 11(3)(c) Data Act.

[51] Along with certain restrictions on use: see Arts. 4(10) and 6(2)(e) Data Act.

terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct".[52] In the case of third parties, there is an additional obligation that sharing data occurs "only to the extent that such disclosure is strictly necessary to fulfil the purpose agreed between the user and the third party".[53]

According to Articles 4(7) and 5(10) of the Data Act, *failure* to agree on "proportionate technical and organizational measures" or to implement them entitles the data holder to *withhold or suspend* sharing the data identified as trade secrets. To prevent this from being an arbitrary decision, the data holder must provide written notice substantiated with reasons to the user/third party and must notify the competent authority pursuant to Article 37 of the Data Act.[54] In addition, the data holder may *refuse access* to data in *exceptional circumstances*, where the data holder "is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organizational measures" taken by the user/third party.[55] It is important to note that such a refusal needs to be notified to the competent authority designated pursuant to Article 37 of the Data Act.

In the case of public sector bodies requesting data to respond to a public emergency, it must be shown that the public sector body is "unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions".[56] For other situations, the public sector body must show that it "has exhausted all other means at its disposal to obtain such data".[57]

In addition, the public sector body must only use the data in a manner compatible with the purpose for which it was requested, "have implemented technical and organizational measures that preserve the confidentiality [...] of the requested data" and erase the data "as soon as they are no longer necessary for the stated purpose".[58] Again, the data holder must identify the data protected as trade secrets and public sector bodies must "take all necessary and appropriate technical and organizational measures to preserve the confidentiality of the

---

[52] Arts. 4(6) and 5(9) Data Act.
[53] Art. 5(9) Data Act.
[54] Arts. 4(7) and 5(10) Data Act.
[55] Arts. 4(8) and 5(11) Data Act.
[56] Art. 15(1)(a) Data Act.
[57] Art. 15(1)(b)(ii) Data Act.
[58] Art. 19(1) Data Act.

trade secrets, including, as appropriate, the use of model contractual terms, technical standards and the application of codes of conduct".[59] The obligations are slightly more onerous on public sector bodies in that the measures must be taken *prior* to the data holder's disclosure of data that is a trade secret, however, the range of measures envisaged is slightly truncated omitting reference to confidentiality agreements and strict access protocols.

Of the obligations mentioned, the requirement that public sector bodies have tried to obtain the data by alternative means is akin to the requirement in compulsory licences for patents of trying to enter into a voluntary licence on reasonable terms and within a reasonable time frame.[60] Further, the requirement to use the data strictly for the requested purpose finds parallels in compulsory licences for patents where "the scope and duration of such use shall be limited to the purpose for which it was authorized".[61] However, the core obligations on users/third parties/public sector bodies relate to preserving confidentiality of data and these are not mirrored in compulsory licences of IPRs. This, as explained above, is because disclosure of the subject matter of an IPR does not threaten its existence, whereas disclosure of the trade secret is likely to destroy the secrecy of the information and its basis for protection. It should therefore come as no surprise that such obligations are created in the case of compulsory licences of trade secrets in the Data Act and, indeed, they are consistent with the types of obligations that are regularly imposed in voluntary licences of trade secrets.[62]

F. Remuneration

Compulsory licences for IPRs usually involve an obligation to pay remuneration to the IPR holder. For example, in the case of patents, Article 31 of TRIPS

---

[59] Art. 19(3) Data Act.

[60] E.g. Art. 31(b) TRIPS.

[61] Art. 31(c) TRIPS.

[62] *Hull*, The licensing of trade secrets and know-how, in: de Werra (ed.), Research Handbook on Intellectual Property Licensing, Edward Elgar 2013, p. 178-179, describes how pure "trade secret/know-how" licences will have a "comprehensive set of confidentiality obligations" along with provisions on use of the information and how it is stored, along with requirements of technical measures (such as passwords, encryption) and organisational measures (such as confidentiality agreements with employees, agents, and others have access to the information).

states that "the right holder shall be paid adequate remuneration in the circumstances of each case, taking into account the economic value of the authorization". In relation to compulsory licences for translations and reproductions of copyright works available to developing countries, Article IV of the Berne Appendix, as well as Articles V(d) and V*quater* 2(b) of the UCC, makes clear that the copyright owner shall receive "just compensation" that is consistent with royalties negotiated in voluntary licences. Note also that Article 13 of Berne permits Union members to grant compulsory licences for re-recordings of musical works (and their associated lyrics) provided, *inter alia*, that this shall not be "prejudicial to the rights of these authors to obtain equitable remuneration".

The Data Act envisages that, in relation to third parties and, in some instances, public sector bodies, compensation will be payable to data holders. In this way, the compulsory licensing of trade secrets in the Data Act is comparable to compulsory licences of IPRs along with voluntary licences of IPRs and trade secrets.[63]

Where the data holder and third parties are in business-to-business relations and data is made available under Article 5 of the Data Act by the data holder, according to Article 8(1) of the Data Act it shall "agree with the data recipient the arrangements for making the data available and shall do so under fair, reasonable and nondiscriminatory terms and conditions and in a transparent manner". How such FRAND conditions will play out is a complex matter and explored elsewhere in this volume.[64] Any agreed compensation, according to Article 9(1) of the Data Act, shall be "non-discriminatory and reasonable and may include a margin". Articles 9(2) and (3) of the Data Act state that the factors that may be taken into account when agreeing on compensation include "costs incurred in making the data available" such as costs for data formatting, electronic storage and dissemination, and "investments in the collection and production of data", along with the "volume, format and nature of the data".

In the case of public sector bodies, Article 20(1) of the Data Act provides that fair compensation will be payable to the data holder where the request is made pursuant to Article 15(1)(b) of the Data Act, i.e. to fulfil "a specific task

---

[63] *Hull*, The licensing of trade secrets and know-how, in: de Werra (ed.), Research Handbook on Intellectual Property Licensing, Edward Elgar 2013, p. 172, 177.

[64] See *Metzger*, Contracts under the Data Act: Review of standard terms and FRAND conditions (Chapter 5 in this volume).

carried out in the public interest, that has been explicitly provided for by law".[65] This compensation "shall cover the technical and organizational costs incurred to comply with the request including, where applicable, the costs of anonymization, pseudonymization, aggregation and of technical adaptation, and a reasonable margin".[66] The basis for these costs will need to be made transparent and if there is disagreement, the public sector body may lodge a complaint with the competent authority designated under Article 37 of the Data Act. While the principle of covering these costs was in the Proposal,[67] the final version specifies examples of type of costs and makes provision for "a reasonable margin". According to Article 9(5) of the Data Act, the Commission is to adopt guidelines on what constitutes reasonable compensation.

There are two instances, however, where data must be made available free of charge under the Data Act. First, to users of connected devices or related services and second, to public sector bodies where the data is necessary to respond to a public emergency, as specified in Article 15(1)(a) of the Data Act, unless the data holder is a microenterprise or small enterprise.[68] While this contrasts with compulsory licences for IPRs, it does not necessarily mean it is impermissible. Instead, it again raises the question of what limitations or conditions, if any, exist for compulsory licences of trade secrets according to TRIPS or whether there is complete discretion to Member States on this matter.

G. State-sanctioned oversight

For compulsory licences of IPRs, usually, there is an application by a third party to a state authority in order to ascertain whether the conditions for grant of a compulsory licence are met. For example, in the case of compulsory licences of patents in the UK, a person must apply to the Comptroller-General of Patents,

---

[65] See Art. 20(2) Data Act. However, Art. 20(4) makes an exception where "the specific task carried out in the public interest is the production of statistics and where the purchase of data is not allowed by national law."

[66] Art. 20(2) Data Act.

[67] European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 22.3.2022, COM/2022/68 final.

[68] Arts. 4(1), 5(1) and 20(1) Data Act.

Designs and Trade Marks.[69] A mechanism of state authority is apparent from Article 31 of TRIPS, which stipulates in relation to patents that any authorization "shall be considered on its individual merits", that any decision relating to the authorization or to any remuneration to be paid for such use "shall be subject to judicial review or other independent review by a distinct higher authority in that Member" and that "the competent authority" should be able to review whether the circumstances justifying the compulsory licence still exist.

The Data Act, however, largely relies on the direct relationships between data holder and user/third party/public sector body. This is because a request for data (which also qualifies as a trade secret) is made by the user, third party or public sector body directly *to* the data holder, rather than via a state authority and it is for the data holder (or trade secret holder, where they are different) to share this data once proportionate technical and organizational measures to maintain confidentiality of the data have been agreed between the parties. That said, there is *some* state sanctioned oversight by virtue of Article 37(1) of the Data Act, which obligates each Member State to designate "one or more competent authorities to be responsible for the application and enforcement of this Regulation". Those competent authorities must have clearly defined tasks and powers, including in relation to "handling complaints arising from alleged infringements of this Regulation, including in relation to trade secrets".[70]

In relation to users and third parties, if the data holder withholds or suspends sharing of data, this must be substantiated in writing to the user/third party without undue delay and notified to the competent authority along with an identification of "which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality undermined".[71] Where there is a refusal to share data because of the likelihood of suffering serious economic damage from the disclosure of trade secrets, despite the technical and organizational measures taken by the user/third party, the data holder must notify the competent authority.[72] A user/third party can lodge a complaint with

---

[69] Ss. 48(1), 130(1) Patents Act 1977 (UK). The Comptroller authorizes officers of the UK Intellectual Property Office to carry out their functions (see s. 74 of the Deregulation and Contracting Out Act 1994 and Manual of Patent Practice guidance on s.130(1) Patents Act 1977 (UK)).

[70] Art. 37(5) Data Act.

[71] Arts. 4(7), 5(10) Data Act.

[72] Arts. 4(8), 5(11) Data Act.

the competent authority about any refusal to share or suspension of sharing, without prejudice to any rights of redress before courts or tribunals.[73]

In the case of public sector bodies, a refusal from the data holder to provide the data requested may be challenged before the competent authority.[74] Meanwhile, the data holder can lodge a complaint to the competent authority if it considers that "its rights under this Chapter have been infringed by the transmission or making available of data" by the public sector body.[75]

In summary, compulsory licensing of trade secrets in the Data Act does entail state sanctioned oversight, however, this occurs *ex post* because the competent authority is functioning largely to restrain arbitrary behaviour by the data holder and to enforce the obligations of data sharing, through requiring notifications and having a complaints mechanism. By way of contrast, in the case of IPRs the oversight is *ex ante* because the state authority determines whether the grant of a compulsory licence is justified and, where it is, issues this licence.

H. Conclusion

It is not a stretch to characterise the data sharing obligations in the Data Act as an example of compulsory licensing of trade secrets. The subject matter of the licence is narrow, given that eligible data are restricted to raw, pre-processed and meta data relating to connected products and services which also qualify as trade secrets within the meaning of the TSD. When it comes to the scope of the licence, it relates to acquisition and use of trade secrets, and this is justified by public interests relating to market failure and instances of exceptional need on the part of public sector bodies. Fair remuneration is due to the data holder, in the case of third parties and public sector bodies that are fulfilling tasks specified by law that are in the public interest, but that do not reach the level of public emergencies. There are obligations on users/third parties/public sector bodies to preserve trade secrets through the adoption of proportionate technical and organisational measures and there is state-sanctioned oversight of the data sharing obligations.

---

[73] Arts. 4(9), 5(12) Data Act.

[74] Art. 18(5) Data Act.

[75] Art. 17(5) Data Act.

The above features are analogous to those we see in compulsory licences of IPRs. To the extent that differences exist, some may be explained by the nature of trade secrets protection as a type of unfair competition protection, rather than as a property right. For example, there is no right of disclosure because this would destroy the trade secret, and the obligations to preserve secrecy are included to reduce this risk. This is also why voluntary licences of trade secrets regularly include obligations of confidentiality and the requirement to adopt precautionary measures to maintain confidentiality. Therefore, it is hard to imagine *any* compulsory licence for trade secrets entitling a user freely to disclose the secret information or omitting obligations on the users to take at least reasonable steps to preserve secrecy. Other differences – such as fair remuneration being required in some but not all instances and *ex post* state oversight – may be down to the lack of explicit guidance in TRIPS, thus apparently leaving wide discretion to TRIPS Members. Arguably, there needs to be further debate about whether TRIPS implicitly places any constraints on compulsory licences of trade secrets and, if so, what these may be. Meanwhile, it will be interesting to observe how the compulsory licensing of trade secrets envisaged by the Data Act plays out in the EU and what other lessons can be learned from this experience.

Chapter 7

Data Act and Data Protection Law

Andreas Sattler*

Starting with its Data Strategy in 2020 it was the aim of the EU-Commission "to create a single European data space [...] where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data [...]".[1] The EU-Commission was convinced that "the value of data lies in its use and re-use", explicitly including "mixed data-sets" which contain personal and non-personal data.[2]

Emphasising a perceived under-use of such data in the EU, the EU-Commission hoped that European data spaces would "foster an ecosystem (of companies, civil society and individuals) creating new products and services based on more accessible data".[3] However, at the same time the EU-Commission left no doubt, that any European data strategy needed to ensure that "European rules and values, in particular personal data protection [...] are fully respected".[4]

Accordingly, Art. 1 (2) DA stipulates that the DA applies to both, personal and non-personal data. Art. 1 (5) s. 1 DA clarifies that the DA "is without prej-

---

* Dr. Andreas Sattler, LL.M., Interim Professor for Law and Informatics, Karlsruhe Institute of Technology (KIT), Germany.

[1] European Commission, A European strategy for data, 19.2.2020, COM(2020) 66 final, p. 6.

[2] European Commission, A European strategy for data, 19.2.2020, COM(2020) 66 final, p. 7.

[3] European Commission, A European strategy for data, 19.2.2020, COM(2020) 66 final, p. 6.

[4] European Commission, A European strategy for data, 19.2.2020, COM(2020) 66 final, p. 6.

udice" to the protection of personal data, privacy and confidentiality of communications as provided for by the GDPR,[5] the Regulation (EU) 2018/1725[6] and the ePrivacy Directive.[7] From Art. 1 (5) s. 3 DA follows that the law on the protection of personal data or privacy shall prevail in the event of a conflict between the DA and the law on the protection of personal data or privacy.[8] According to Art. 1 (5) s. 2 DA the DA shall complement the right of access stipulated by Art. 15 GDPR and the right to data portability under Art. 20 GDPR if the data subjects are at the same time Users as defined by Art. 2 No. 12 DA. Thus, there seems to be clear guidelines on the relationship between the Data Act and the GDPR. However, once the obligation to make product data and related service data accessible to the User (Art. 3 DA), and the User's right to access, use and make personal data available according to Art. 4 and Art. 5 DA are analysed, this first impression starts to crumble. It becomes obvious that the objectives pursued with the DA will potentially shatter on the rocks of the GDPR (A).

If the DA is meant to be successful as regards personal data, this requires an interpretation and application of the GDPR that is supportive of these rights to access, use and share data (B).

---

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

[6] Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

[7] Directive 2002/58/EC of 12.07.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[8] The rule in the event of conflict had been demanded by the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB): EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access and use of data, 4.5.2022, p. 7.

A. The interfaces between DA and GDPR

According to the understanding of the European legislator it – presumably – seemed to suffice to provide for a general rule to avoid overlaps and conflicts between the DA and the GDPR (I). As far as the data subject's right to information (Art. 15 GDPR) and the right to portability (Art. 20 GDPR) are concerned, the DA contains an explicit modification (II). However, when turning to the principle of accessibility by design in Art. 3 DA, a (first) fundamental tension between the objectives of the DA and the GDPR becomes obvious (III).

I. General rule: Prevailing of the GDPR

At first glance the relationship between DA and GDPR seems to follow an unambiguous rule. According to Art. 1 (5) s. 1 the DA "is without prejudice" to the law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, in particular the GDPR, the Regulation (EU) 2018/1725[9] and the ePrivacy Directive.[10] In the event of a conflict between DA and the aforementioned laws on the protection of personal data or privacy the latter "shall prevail", Art. 1 (5) s. 3 DA.

Moreover, in the context of both, the right to access and use data and the right to share data, Art. 4 (12) DA and Art. 5 (7) DA require a valid legal basis according to Art. 6 GDPR for any processing of personal data in case the User is not the data subject whose personal data is requested.[11] Rather redundantly Art. 5 (13) DA stipulates that the right to share data with a third party shall not adversely affect the rights of data subjects pursuant to the law on the protection of personal data.

While Art. 4 (12) and Art. 5 (7) DA merely point towards Art. 6 GDPR, Rec. 7 s. 7 and s. 10 DA clarify that the DA "does not constitute a legal basis for the collection or generation of personal data by the data holder" nor "create a legal basis for providing access to personal data or for making personal data available to a third party" in case the User is not the data subject. Consequently, and in

---

[9] Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, OJ L 295, 21.11.2018, p. 39–98.

[10] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

[11] See also: Rec. 7 s. 6 DA.

contrast to the EU-Commission's Proposal, it becomes clear from the final wording, that Art. 4 (1) and Art. 5 (1) DA provide no legal bases for the processing of personal data outside the GDPR nor is it likely that Art. 4 (1) and Art. 5 (1) DA complement the opening clauses according Art. 6 (1) lit. c, lit. e GDPR and Art. 9 (2) lit. g GDPR (see below Section B.II.1.c).

II. Modification of Art. 15 and Art. 20 GDPR

While Art. 1 (5) s. 1 and s. 3 DA reinforce the GDPR as the sole building block as regards the processing of personal data, contrastingly, Art. 1 (5) s. 2 DA stipulates that the right to access and use data (Art. 4 DA) and the right to share data (Art. 5 DA) "shall complement" the right to access and the right to portability assigned to data subjects by Art. 15 and Art. 20 GDPR respectively.

The extent of this "complementation" – which actually amounts to a substantive reform[12] – only becomes obvious against the background of the obstacles that are inherent to Art. 15 and Art. 20 GDPR. According to Art. 20 (1) GDPR the right to port data to another controller requires that the processing of data had been carried out by automated means and had been based either on consent (Art. 6 (1) lit. a GDPR) or on a (pre-)contractual relationship with the data subject (Art. 6 (1) lit. b GDPR).[13] Therefore, Art. 20 GDPR is not applicable in cases where the data has been collected by non-automated means nor if the processing was based on a legitimate interest (Art. 6 (1) lit. f GDPR).

Departing from these requirements, Rec. 35 s. 6 DA explains that Art. 4 (1) and Art. 5 (1) DA grant a User the right to access data and make it available to a third party "irrespective of their nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing". Furthermore, Rec. 35 s. 7 DA clarifies that the DA guarantees the technical feasibility of third parties' access to all types of data falling within its scope. This modification of Art. 20 (2) GDPR[14] ensures that technical obstacles no longer hinder or prevent such access to personal data. While the rights of the Users remain free of charge,[15] the DA allows Data Holders to charge

---

[12] While such a reform is to be welcomed, it nevertheless, would be preferable if it took place within Art. 15 and Art. 20 GDPR. However, such a change seems to be impossible for political reasons.

[13] See also Rec. 68 s. 4 GDPR.

[14] See also Rec. 68 s. 10 GDPR.

[15] Art. 4 (1) and Art. 5 (1) DA.

third parties a reasonable compensation in order to cover for costs incurred when providing direct access to the data generated by a connected product, Rec. 35 s. 8 DA. Though Art. 5 (1) DA deliberately modifies the right to port personal data to a third party according to Art. 20 GDPR, Art. 5 (8) DA clarifies that a failure of a Data Holder and a third party to agree on the terms for such sharing does not prevent the data subject from exercising its right under Art. 20 GDPR.[16]

This modification of Art. 20 GDPR raises two questions. *Firstly*, it is must be decided whether Art. 4 (1) and Art. 5 (1) DA allow for a transfer of the data or whether both norms merely provide a so-called "in situ right" (1). *Secondly*, the DA provides for a more restrictive model as regards gatekeepers. This is meant to exclude the operators of powerful platforms from the benefits of Art. 4 and Art. 5 DA. However, this exemption raises the question of whether such restrictions should have repercussions on the application of Art. 20 GDPR if personal data is ported to a gatekeeper (2).

1. Comprehensive right to access or mere *in situ right*

With regard to the EU-Commission's Proposal of the DA it was unclear, whether the right to access data provided merely a so-called *in situ right* or a comprehensive right to data portability.[17] The former would limit the benefits of data access fundamentally as it would only allow an analysis of the data under the persisting control of the Data Holder. An interpretation according to which Art. 3–5 DA would only oblige the Data Holder to offer such *in situ rights* stems from the vague wording in Rec. 22 DA.

According to Rec. 22 s. 6 DA connected products "may be designed to permit the user or a third party to process the data on the connected product, on a computing instance of the manufacturer or within an information and communications technology (ICT) environment chosen by the user or the third party." However, when read in conjunction with sentences 1–3 it becomes obvious that Rec. 22 DA only mentions examples of how the data may be accessed by Users

[16] See also Rec. 35 s. 9 DA.

[17] *Kerber*, Governance of IoT-Data: Why the EU Data Act Will Not Fulfill Its Objectives, GRUR Int. 2023, 120 (124).

and third parties. As Art. 4 (1) and Art. 5 (1) DA are explicitly intended to complement the right to portability in Art. 20 GDPR,[18] granting merely an *in situ right* would jeopardise this objective of the DA. Moreover, considering its tentative language („may"), it is not even convincing to interpret Rec. 22 as an expression of the EU legislator's will that an *in situ right* should suffice as regards an access to realtime data.[19]

However, when compared to a comprehensive right to port or transmit the data to a third party, an *in situ right* offers a less intrusive measure. Therefore, it could provide a solution in cases where granting a right to transmit such data would risk that the Data Holder or the User loses a trade secret. Furthermore an *in situ right* could be regarded as a proportionate measure in individual cases as it reduces the risk of violating the privacy of data subjects or the confidentiality of communication. Especially when balancing the legitimate interest of a controller and the interests, rights and freedoms of a data subject, providing merely an *in situ right* as remedy might tip the assessment of Art. 6 (1) lit. f GDPR in the controller's favour.

2. Repercussions of Art. 4 and 5 DA on Art. 20 GDPR

As unambiguously stated by Art. 1 (5) and Art. 5 (8) and (13) DA the rights according to Art. 4 and Art. 5 DA shall not hinder or prevent the data subject from exercising its right under Art. 20 GDPR. However, the DA might have a reverse effect on Art. 20 GDPR. Starting with its Digital Market Act (DMA),[20] the EU legislator has opted for an asymmetric regulatory framework that enables a tighter regulation of gatekeepers.[21] According to Art. 3 DMA an undertaking shall be designated as a gatekeeper if it has a significant impact on the internal

---

[18] *Perarnaud/Fanni*, The EU Data Act – Towards a new European data revolution?, CEPS Policy Insights No 2022-05, 2022, S. 4, available at https://www.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-05_The-EU-Data-Act.pdf (28.2.2024); *Steinrötter*, Verhältnis von Data Act und DS-GVO, GRUR 2023, 216 (221).

[19] In this direction and making the point that Art. 20 GDPR does not provide for the portability of real-time data: *Specht-Riemenschneider*, Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, ZEuP 2023, 638 (669).

[20] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L 265, 12.10.2022, p. 1–66.

[21] For the relationship between DMA and DA: *Weck*, The EU Data Act – The Interface with Competition Law, Section C (Chapter 3 in this volume) and *Martens*, A comparative economic perspective on EU data market regulations, Section D (Chapter 2 in this volume).

market, if it provides a core platform service which is an important gateway for business users to reach end users and if it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

When discussions on the DA were originally initiated, it was already clear that the right to access, use and share data should not be available to such gatekeepers. This was based on the assumption that accepting gatekeepers as beneficiaries of these rights would only foster their already strong market position. Thus, Art. 5 (3) DA stipulates that gatekeepers shall not be an eligible third party under Art. 5 DA and, therefore, shall not solicit or commercially incentivise a User in any manner to make such data available to one of the gatekeeper's services that the User has obtained pursuant to a request under Art. 4 (1) or Art. 5 (1) DA. This prohibition is extended to other third parties according to Art. 6 (2) lit. d DA, thus, barring the latter from making the received data available to gatekeepers.

Rec. 40 DA explains this exclusion of gatekeepers as data recipients due to their unrivalled ability to acquire data. According to Rec. 40 s. 6 DA including gatekeeper as beneficiaries of the data access right would be disproportionate for Data Holders, who are subject to these obligations. Moreover, Rec. 40 s. 9 DA clarifies that third parties to whom data is made available at the request of the User may not – via subcontracting – make the data available to a gatekeeper. However, as *Wolfgang Kerber* highlighted, the DA does not explicitly prohibit factual or legal arrangements according to which a Data Holder transfers its position to a new Data Holder, who is a gatekeeper.[22]

With this intention of the DA in mind, it seems convincing to employ the same limitation when applying Art. 20 (1) GDPR and its right of the data subject to transmit personal data to another controller, where the latter is a gatekeeper. Put short: If the new controller is a gatekeeper according to Art. 3 DMA

[22] Presentation on "Developing the Data Act: Market Failures, Value of Data, and Consumer Choice in the B2C Sector" by *Wolfgang Kerber* at the conference on "The Value of Consumer Data in the Digital Economy" 18/19.4.2024, University of Ferrara, Italy. Such a transfer of the position as data holder might – at first glance – be regarded as a situation which is comparable to the sharing with a Data Recipient, thus, allowing for an analogue application of Art. 5–9 and Art. 13 DA. However, Rec. 40 s. 14 DA argues against such an analogy as "voluntary agreements between gatekeepers and data holders remain unaffected [and] the limitation on granting access to gatekeepers would not exclude them from the market or prevent them from offering their services."

then Art. 20 (1) GDPR should be interpreted as restrictively as Art. 4 and Art. 5 DA. As the latter are supposed to complement Art. 20 GDPR it seems convincing to extend the objective of Art. 5 (3) DA and Art. 6 (2) lit. d DA to Art. 20 GDPR. However, while such an extensive interpretation of the exclusion of gatekeepers appears to be consistent with the current regulatory trend it, nevertheless, conflicts with Rec. 40 s. 12 DA. Hereafter, the exclusion of gatekeepers from the benefits of Art. 4 and Art. 5 DA does not "prevent those undertakings from obtaining and using the same data through other lawful means." Consequently, it seems to be the intention of the EU legislator to allow gatekeepers to incentive data subjects to employ Art. 20 (1) GDPR and thus port the data to the gatekeeper as the new controller. Unless the *CJEU* holds such instrumental use of Art. 20 GDPR to be a circumvention of Art. 5 (3) DA, Art. 20 GDPR must be qualified as such "other lawful means" according to Rec. 40 s. 12 DA.

III. Accessibility by design versus privacy by design

While the modification of Art. 15 and Art. 20 GDPR by way of Art. 4 and Art. 5 DA may seem to cause only minor tensions between the DA and the GDPR, this picture changes once Art. 3 DA and its principle of accessibility by design comes into play (1). Such principle collides with the GDPR's principles of data minimisation and privacy by design (2). However, the EU legislator has paid little attention to this conflict (3).

1. Data Act: Accessibilty by design

According to Art. 3 (1) DA the manufacturers of connected products and the providers of related services shall design their products and provide their services in such a manner that data generated by their use are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the User. This includes metadata[23] that is necessary for the interpretation and use of such data. Whilst most obligations of the DA address Data Holders, Art.

[23] According to Art. 2 (2) DA, 'metadata' means a structured description of the contents or the use of data facilitating the discovery or use of that data.

3 DA addresses the manufacturers of connected products[24] and the providers of related services[25] and thus focuses on the starting point of most data supply chains.

Rec. 15 DA clarifies that Art. 3 (1) DA includes data which represents "user actions and events", including data which result indirectly from the User's action,[26] all data indicating hardware status and malfunctions[27] and even data generated during times of inaction by the User.[28] However, according to Rec. 20 S. 5 DA the data covered by Art. 3 (1) DA seems to be limited to "readily available data". Art. 2 no. 17 DA defines "readily available data" as product data[29] and related service data[30] that a Data Holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation. Despite the fact, that the term "readily availa-

---

[24] According to Art. 2 (5) DA, 'connected product' means 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, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user.

[25] According to Art. 2 (6) DA, 'related service' means a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product.

[26] Rec. 15 s. 5.

[27] Rec. 15 s. 6.

[28] Rec. 15 s. 7 ("in stand-by mode or even switched off, as the status of a connected product or its components, for example its batteries, can vary when the connected product is in stand-by mode or switched off").

[29] According to Art. 2 (15) DA, "product data" means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer.

[30] According to Art. 2 (16) DA, "related service data" means data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider.

ble data" – it is predominately used in the context of Chapter VI DA ("Switching between Data Processing Services") – Rec. 20 S. 5 DA, nevertheless, introduces this term in the context of Art. 3 DA.[31]

According to Rec. 20 S. 6 DA the term "readily available data" does not include data generated by the use of a connected product where the design of the connected product does not provide for such data being stored or transmitted outside the component in which they are generated or the connected product as a whole. Consequently, the term "readily available data" is crucial for the scope of Art. 3 (1) DA.[32] As becomes only apparent from Rec. 20 S. 7 DA, Art. 3 (1) DA itself "does not impose an obligation to store data on the central computing unit of a connected product".[33] However, it remains unclear whether Rec. 20 S. 7 DA refers to the manufacturers of connected products and the providers of related services (Art. 3), whether is concerns the duties of the Data Holder according to Art. 4 DA or both.

2. GDPR: Data minimisation and privacy by design

Whilst Art. 3 DA corresponds with the crucial aim of the DA to enable access to data and to facilitate the use and sharing of such data it, nevertheless, clashes – at least – with two principles of the GDPR.

Firstly, Art. 5 (1) lit. c GDPR stipulates that the processing of personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

Secondly, according to Art. 5 (1) lit. g GDPR personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Storage for a longer period is acceptable insofar as the personal data will be processed solely

---

[31] The term is used in the context of the pre-contractual information duties of a provider of related service towards the user, Art. 3 (3) lit. c DA.

[32] Rec. 20 DA seems to be a hybrid as it refers predominately to the designing and manufacturing of connected products the designing and provision of related services and thus to the obligations stipulated in Art. 3 DA. However, Rec. 20 s. 5 DA focuses on the role of the Data Holder and his ability to grant access to data.

[33] Contrastingly, Rec. 20 S. 9 DA leaves it to future Union or national law "to outline further specificities, such as the product data that should be accessible from connected products or related services, given that such data may be essential for the efficient operation, repair or maintenance of those connected products or related services".

for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, Art. 89 (1) GDPR ('storage limitation'). As Art. 89 (1) GDPR requires a public interest it does not allow private companies to store such data merely because innovation by private companies might correspond with a general public interest, too. As the *CJEU* has emphasised in the context of Art. 6 (1) lit. e GDPR (data processing in a public interest) "it seems unlikely that [Meta as] private operator was entrusted with such a task" of carrying out research for the social good in the public interest, if its activities are essentially of economic and commercial nature.[34]

As a flanking measure to these principles, Art. 25 GDPR stipulates that the controller shall implement appropriate technical and organisational measures (TOMs) to ensure that, by default, only personal data which is necessary for each specific purpose is processed. This obligation applies to the *amount* of personal data collected, the *extent* of its processing, the *period* of its storage and its *accessibility*. Additionally, the controller shall implement measures that ensure, by default, that personal data is not made accessible to an indefinite number of persons without the individual's intervention (data protection by design and by default). Whilst it is not impossible to synchronise Art. 5 (1) lit. c, lit. g and Art. 25 GDPR and Art. 3 (1) DA, nevertheless, the underlying tensions are obvious.[35] In a Joint Opinion on the Proposal of the DA the *European Data Protection Supervisor* (EDPS) and the *European Data Protection Board* (EDPB) have criticised this approach. It seems to be a direct reaction to this criticism[36] that the EU legislator has included Rec. 20 s. 9 DA. It states that the design obligations in Art. 3 DA are "without prejudice to the data minimisation principle" as described in Article 5 (1) lit. c GDPR. Thus, Art. 3 DA "should not be understood as an obligation to design products and related services in such a way that they process or store any personal data besides what is necessary in relation

---

[34] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 133.

[35] According to Rec. 8 S. 3 DA, all parties to data sharing should use pseudonymisation, encryption and technology that permits algorithms to be brought to the data and allow valuable insights to be derived without the transmission of the analysed data.

[36] EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access and use of data, 4.5.2022, p. 7.

to the purposes for which they are processed".[37] However, research and innovation based on use and re-use of personal data is open-ended and thus difficult to reconcile with the principles of data minimisation, storage limitation and purpose limitation.[38]

3. Weak attempts to synchronize the DA and the GDPR

Art. 3 (1) DA and Art. 5 GDPR clearly lead to a conflict of objectives. The EU legislator tried to mitigate this conflict in Art. 4 (5) and Art. 5 (4) DA. When verifying whether a User's request for data access (Art. 4 DA) or for making data available (Art. 5 DA) is qualified, Data Holders shall not require that person to provide any information beyond what is necessary for such verification. Furthermore, Data holders shall not keep any information on the User's or third party's request for access beyond what is necessary for the sound execution of the request. Moreover, Rec. 21 s. 4 and Rec. 29 s. 1 DA suggest that Users and Data Holders rely on user accounts as a means of communication and to submit and process data access requests. However, while such user accounts could provide an effective tool to verify a User's entitlement to request access, use or to make data available, it, nevertheless, results in an expansion of personal data as all data covered by such a request will be related to the requesting User, in case the User is a natural person.

Although it is obviously the purpose of Art. 4 (5) and Art. 5 (4) DA to emphasise that only such personal data should be processed that is strictly necessary, such a stipulation might indeed backfire as it incentivizes Data Holders to implement individual user accounts and disincentivizes other solutions such as anonymisation or relying on data intermediaries and Personal Information Management Systems (PIMS).[39] Consequently, the fundamental conflict between DA and GDPR persists.

---

[37] According to Rec. 24 s. 6, the data holder "should implement a reasonable data retention policy, where applicable, in line with storage limitation principle pursuant [Article 5 (1), lit. e GDPR], that allows for the effective application of the data access rights provided for in this Regulation."

[38] Art. 5 (1) lit. b GDPR. In this regard see below: Section C.III.3.

[39] According to Rec. 33 s. 6 DA, data intermediaries and PIMS are considered as useful tool when establishing commercial relations between Users and third parties, especially for the purpose of aggregating access to data so that big data analyses or machine learning can be facilitated.

B. Future synchronisations of DA and GDPR

As has been shown, the DA does not provide for a satisfying synchronisation. Contrastingly, the general objectives of the DA and in particularly the concept of accessibility by design (Art. 3 (1) DA) clashes with the objectives of the GDPR.[40] As the DA is without prejudice to the application of the GDPR and as the latter prevails over the DA in case of conflict, the interpretation of the GDPR by the judiciary and thus, eventually by the *CJEU* will decide whether the DA will actually have a positive impact on data-driven innovation or whether the DA will prove to be a paper tiger. As the DA imports fundamental legal uncertainties inherent to the GDPR, the DA's impact on facilitating data markets and data-based innovation is additionally endangered (I). The potential of the DA will depend on the options that Art. 6 GDPR provides for the processing of personal data (II). As if this was not already challenging, the following analysis shows that it is the interpretation of the requirements for valid consent that will eventually decide on the success or failure of the DA as far as (sensitive) personal data of a multitude of data subjects is concerned (III).

I. Importing legal uncertainty from the GDPR

Apart from trade secret protection, the protection of personal data is the second major obstacle to the creation and functioning of European data markets. As with other Acts that are meant to facilitate such data markets, the DA leaves the GDPR generally unchanged. Negotiations on the DA have not led to a (necessary) overhaul of other European Acts that profoundly deter the development of data-based innovation based on efficient and effective accessibility of such data.[41]

---

[40] This should not ignore the fact that Art. 1 (3) GDPR promotes the free movement of personal data within the Union, thus allowing an interpretation of the GDPR that promotes the objections of the DA.

[41] See for the challenges to design a functioning bundle of rights: *Eckardt/Kerber*, Designing the Bundle of Rights on IoT Data: The EU Data Act, Sections C and D (Chapter 1 in this volume); for an alternative and economically superior solution in the EU Health Data Space: *Martens*, A comparative economic perspective on EU data market regulations, Section B (Chapter 2 in this volume); for the challenges posed by the interface of Art. 43 DA and the protection of databases: *Wiebe*, The Database Right and Art. 43 of the Data Act, Sections B and C (Chapter 9 in this volume).

When the GDPR was drafted a decade ago, the challenges and the opportunities stemming from technical developments such as AI and IoT were hardly anticipated. It is always a challenge for controllers to decide which data is personal or even sensitive. This challenge is hardly bearable in the context of IoT scenarios. The legal uncertainty roots in the broad definition of both, personal data (1) and special categories of data (2).

1. Personal Data

According to Art. 4 no. 1 GDPR personal data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one, who can be identified, directly or indirectly. According to the *CJEU*, data is to be treated as personal data once a potential controller has a right to information against a third party and if such information received from a third party enables the controller to identify a data subject.[42] However, in the same judgement the *CJEU* introduced a threshold for such identification if it is "practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[43] Consequently, the distinction between non-personal data and personal data depends on the "legal means" available to a potential controller and whether such identification requires merely such efforts which seem proportionate.[44] Thus, the definition of personal data provides no sharp delineation but, instead, leads into an area of shades of grey.

2. Sensitive Personal Data

Once personal data is included, controllers immediately enter the next notoriously grey area. Distinguishing between data that merely identifies a data subject

---

[42] CJEU, Judgement of 19.10.2016, Breyer/Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779, para. 49: "a dynamic IP address registered by an online media services provider when a person accesses a website [...] constitutes personal data [...] in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person".

[43] CJEU, Judgement of 19.10.2016, Breyer/Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779, para. 46.

[44] It remains unclear how such proportionality will be assessed and whether it relates to the value of identification for the particular controller or whether an objective value will be applied.

and such data that entails particularly sensitive categories of data as defined by Art. 9 (1) GDPR is virtually untenable. It is typically beyond the influence of a Data Holder whether or not a User, who is a data subject provides data or acts in a manner that (automatically) generates data[45] which contains information that falls under the category of sensitive data.

However, if a set of data contains both sensitive personal data and non-sensitive personal data and if such data is collected *en bloc* and, thus, without a chance to separate personal and sensitive personal data from each other at the time of collection, Art. 9 (1) GDPR applies. Consequently, any processing of a data set is prohibited, if it contains at least one sensitive data item and none of the derogations in Art. 9 (2) GDPR are applicable.[46]

As the *CJEU's Grand Chamber* decided in 2023, data sets typically contain a sensitive data item where the user of an online network visits websites or apps to which one or more of the categories referred to in Art. 9 (1) GDPR relate and if the user enters information into them when registering or when placing online orders.[47] It is for example sufficient that the operator of an online network collects – by means of integrated interfaces, cookies or similar storage technologies – data on a user's visit to sites and apps and of the information entered by the user on such sites or apps that allow conclusions to be drawn as to the sexual or religious orientation of the user.[48] According to the *CJEU* it is irrelevant whether or not the information revealed by the processing is correct and whether or not the controller is acting with the aim of obtaining such sensitive data.[49]

Consequently, the linking of such data with a user's network account and the use of such data by the network operator, must be regarded as processing of

---

[45] Once again it is important to notice that according to Art. 3 (1) DA connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data are – by default – directly accessible to the user. See also Rec. 15 DA.

[46] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 89.

[47] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 73.

[48] See also: CJEU, Judgement of 1.8.2022, Vyriausioji tarnybinės etikos komisij, C-184/20, ECLI:EU:C:2022:601, para. 124-128.

[49] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 69.

special categories of personal data (sensitive data). As soon as connected products or related services – such as fitness trackers or health apps – generate personal data on physical or physiological functions, processing of such data is in principle prohibited unless one or more of the derogations provided for in Article 9 (2) GDPR apply.

In the same judgement the *CJEU* expressed the opinion that operators of such networks are typically barred from processing such sensitive data based on Art. 9 (2) lit. e GDPR. According to the court a user does not manifestly make sensitive data publicly available merely by visiting websites or apps to which one or more of the categories set out in Art. 9 (1) GDPR relate. Thus, if an online network or the provider of a connected product or related services wishes to collect data relating to those visits via cookies or similar storage technologies, it cannot rely on Art. 9 (2) lit. e GDPR[50] but, contrastingly, requires another legal basis. At least in a private law context such legal basis is typically the *explicit* consent of all data subjects involved. However, the necessity to rely on consent poses fundamental challenges (see below Section B.III.).

II. Applicable legal bases

The *EU-Commission's* initial Proposal of the DA and Art. 1 (5) DA leave some room for an interpretation according to which the right to access, use and share data constitute additional legal bases outside the GDPR.[51] However, the final wording of Rec. 7 DA unambiguously states that the DA "does not constitute a legal basis for the collection or generation of personal data by the data holder"[52] nor "does [it] create a legal basis for providing access to personal data" where the User is not the data subject.[53] Instead, any access, use and sharing of personal

---

[50] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 84. For Art. 9 (2) lit.e to be applicable, the data subject must have explicitly made the choice beforehand, for example on the basis of individual settings selected with full knowledge of the facts and by hereafter clicking or tapping on those "Like-Buttons" or "Share Buttons".

[51] In favour of such an interpretation in the context of the Council's Mandate: *Specht-Riemenschneider*, Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, ZEuP 2023, 638 (665 ss.).

[52] Rec. 7 s. 7 DA.

[53] Rec. 7 s. 10 DA.

data requires a valid legal basis under Art. 6 GDPR and where sensitive personal data is concerned, in accordance with the conditions of Art. 9 GDPR.[54]

Consequently, the interpretation and application of the GDPR will essentially decide whether or not the objectives of the DA will be achieved or whether the rights to access, use and share of data will wreck on the rocks of the GDPR. Therefore, it is essential to explore the potential of the legal bases provided by Art. 6 GDPR in the context of Art. 4 and Art. 5 DA (1). A subsequent analysis of Art. 6 (2) lit. b DA confirms that the DA constitutes no legal basis for the processing of personal data (2).

1. Application of Art. 6 GDPR

According to Art. 4 (13) s. 1 and Art. 4 (14) DA a Data Holder shall only use readily available data that is non-personal data and shall only make such data available to a third party on the basis of a contract with the User. This requirement corresponds with the legislator's approach to place the User at the center of all data innovation chains.[55] Yet, it is surprising that non-personal data can only be used and shared based on a contract whereas personal data can – in general – be processed based on several legal bases provided by Art. 6 (1) GDPR.

When exploring the legal bases provided by the GDPR it is crucial to recall that Art. 6 (1) GDPR constitutes "an exhaustive and restrictive list"[56] of the cases in which processing of personal data can be regarded as lawful. Although all derogations in Art. 6 (1) GDPR can enable the processing of personal data, it will subsequently become obvious that consent takes priority.[57] Consequently, it is no exaggeration to assume that the success of the DA – as far as

---

[54] Rec. 7 s. 6 and s. 11 DA.

[55] This User centric approach is reinforced by Art. 6 (2) lit. c DA according to which the third party shall not make the data it receives available to another third party, unless the data is made available on the basis of a contract with the User.

[56] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 90; CJEU, Judgment of 22.6.2021, Latvijas Republikas Saeima (Penalty points), C-439/19, ECLI:EU:C:2021:504, para. 99.

[57] *Sattler*, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 GDPR, in: Lohsse/Schulze/Staudenmayer (eds.), Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V, 2020, p. 223 ss.; *Sattler*, Informationelle Privatautomomie, 2022, p. 277 ss., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

personal data is concerned – will eventually depend on consent and the efficient administering of a cascade of consents by the data subjects via PIMS. This interdependency between the DA and consent becomes obvious once the limitations of the potential alternative legal bases have been identified.

a) Art. 6 (1) lit. b GDPR: Necessity for the performance of a contract

According to Art. 6 (1) lit. b GDPR the processing of personal data shall be lawful if it "is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". At first glance Art. 6 (1) lit. b GDPR seems to be a perfect match with Art. 4 (13) s. 1 and Art. 4 (14) DA which require a contract between User and Data Holder as far as non-personal data is used or shared. However, the *CJEU's Grand Chamber* decided that consent takes priority and, therefore, Art. 6 (1) lit. b GDPR "must be interpreted restrictively", as it allows a lawful processing of personal data in the absence of the data subject's consent.[58] Moreover, the *CJEU* ruled that the processing of personal data is only necessary for the performance of a contract, if it is objectively indispensable for a purpose that is integral to the contractual obligation.[59] This is only the case where the processing is essential for the proper performance of the contract concluded between the controller and the data subject, meaning that there "are no workable, less intrusive alternatives" available.[60]

This reasoning seems to support an interpretation according to which Art. 6 (1) lit. b GDPR predominantly provides a tool to decrease the pressure on data subjects to make decisions. Where a controller and a data subject have entered into contract or where the data subject plans to do so, it would be unreasonably burdensome to require a data subject's consent and, thus, exhaust the data subject's capacity of decision making.[61] This relief function of Art. 6 (1) lit. b

---

[58] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 93; see also: CJEU, Judgment of 24.2.2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, para. 73.

[59] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 98.

[60] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 99.

[61] *Sattler*, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 I GDPR, in: Lohsse/Schulze/Staudenmayer (eds.), Data as Counter-Performance – Contract

GDPR and the requirement that such processing is indispensable for a purpose that is integral to the contractual obligation limits its applicability to circumstantial data processing such as bank details and postal addresses in sale contracts. Consequently, Art. 6 (1) lit. b GDPR provides no legal basis when personal data is either commercialised for personalised advertising or processed to provide a data subject with individualised smart services or smart products.[62] Therefore, Art. 6 (1) lit. b GDPR seems unsuitable to legitimise the processing of personal data in the context of Art. 4 and Art. 5 DA when the request for access, use and sharing of such data is made by a User. This is despite Rec. 34 s. 8 DA, which states that a User, who as controller intends to request personal data generated by the use of a connected product or related service is required to have a legal basis for processing the data, "such as [...] the performance of a contract to which the data subject is a party".

b) Art. 6 (1) lit. f GDPR: Processing as legitimate interest

Art. 6 (1) lit. f GDPR allows to process personal data if it is necessary for the purposes of a legitimate interest pursued by the controller or by a third party, except where such interest is overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child.

Law 2.0? Münster Colloquia on EU Law and the Digital Economy V, 2020, p. 223 (241 s); *Sattler*, Informationelle Privatautomomie, 2022, p. 287 ss., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

[62] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 102. The CJEU concludes that although a personalisation of the services by Meta is useful to the user, as it enables the user to view content corresponding to a large extent to his or her interests, such personalisation does, nevertheless, not appear to be necessary in order to offer that user the services of the online social network. Contrastingly, such services may be provided to the user in the form of an equivalent alternative which does not involve such a personalisation. Arguably of a different opinion was the European Data Protection Board (EDPB), which stated in the context of the Digital-Content-Directive that "personalisation of content may (but does not always) constitute an expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases". EDPB, Guidelines 2/2019 on the processing of personal data under Art. 6 (1) (b) GDPR in the context of the provision of online services to data subjects, 16.10.2019, para. 54.

The objectives of the DA in general and the rights according to Art. 4 (1) and 5 (1) DA in particular must be understood as a statement in favour of the accessibility, the use and the sharing of personal data. This suggests that the rights constituted by Art. 4 (1) and Art. 5 (1) DA can be regarded as important legitimate interests in the context of Art. 6 (1) lit. f GDPR. Consequently, Art. 6 (1) lit. f GDPR might become an important legal basis within the scope of the DA.[63] Otherwise those rights which are granted to a User, irrespectively of whether or not the User is identical to the data subject, would always be depending on an active opt-in of the data subject.[64] If the processing of personal data to satisfy the rights of the User, who is not the data subject, could not be based on Art. 6 (1) lit. f GDPR, any access, use and sharing of such data would either require the data subject's consent according to Art. 6 (1) lit. a GDPR or a contract with the data subject according to Art. 6 (1) lit. b GDPR.

However, if Art. 6 (1) lit. f GDPR is intended to be an important legal basis under the DA, the EU legislator should have stated so unmistakably. Instead, the DA only insufficiently elaborates on the relationship between Art. 4, Art. 5 DA and Art. 6 GDPR in general and Art. 6 (1) lit. f GDPR in particular.[65] Indeed, when referring to the *Council's Mandate* for negotiations with the European Parliament ("Council's Mandate"),[66] it becomes doubtful, whether Art. 6 (1) lit. f GDPR is applicable within the scope of the DA.

According to Rec. 30 s. 8 of the *EU-Commission's Proposal*[67] a User requires a legal basis for processing the data "such as the consent of the data subject or *legitimate interest*".[68] However, following a demand by the *Council's Mandate*, Rec. 30 s. 8 was changed. Therefore, the final wording of – now – Rec. 34 s. 8

---

[63] Similar: *Hennemann/Steinrötter*, Der Data Act, NJW 2024, 1 (6); *Specht-Riemenschneider*, Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, ZEuP 2023, 638 (667).

[64] In contrast to Art. 6 (1) lit. a (consent) and lit. b GDPR (contract), Art. 6 (1) lit. f GDPR leaves the decision to the controller and provides the data subject only with an opt-out according to Art. 21 (1) GDPR.

[65] See also: Position Paper of the German Bar Association on the Proposal for a Regulation on harmonised rules on fair access, July 2022, p. 5 s., available at https://anwaltverein.de/de/newsroom/sn-40-22-vorschlag-der-eu-kommission-fuer-ein-datengesetz (28.2.2024).

[66] Council of the European Union, Interinstitutional File of 17.3.2023: 2022/0047(COD).

[67] European Commission, Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), 22.3.2022, COM(2022)68 final.

[68] Emphasis added.

DA states, that a User, who as controller intends to request personal data generated by the use of a connected product or related service is required to have a legal basis for processing the data, "such as the consent of the data subject or the *performance of a contract* to which the data subject is a party".[69] Put short: The negotiations between *Council* and *Parliament* led to the substitution of a reference to Art. 6 (1) lit. f GDPR by a reference to Art. 6 (1) lit. b GDPR.

Rec. 34 s. 9 DA still requires that the User should ensure that the data subject is informed of the "specified, explicit and *legitimate purposes* for processing those data".[70] However, this wording refers to the principle of purpose limitation according to Art. 5 (1) lit. b GDPR and not to the *legitimate interest* in Art. 6 (1) lit. f GDPR.

Despite such an apparent alteration of its wording during the negotiations, Rec. 34 DA cannot be interpreted as an exclusion of Art. 6 (1) lit. f GDPR in the context of Art. 4 (1) and Art. 5 (1) DA. *Firstly*, recitals can only supplement the statutory provisions and are thus of a non-binding nature. *Secondly*, while Rec. 34 s. 8 DA mentions consent and contract explicitly, it does so only to provide examples of legal bases for the processing of personal data ("such as"). Thus, the modification of the wording of Rec. 34 DA demonstrate a poor understanding of the interfaces between DA and GDPR rather than a carefully balanced attempt to synchronise both European Acts.

However, assuming – rightly so – that Art. 6 (1) lit. f GDPR is a valid legal basis in the context of Art. 4 (1) and Art. 5 (1) GDPR then its potentially vast scope turns it into the "loose cannon" on board of the DA. Put positively: Art. 6 (1) lit. f GDPR allows for a cautious balancing of the User's or third party's legitimate interests on the one side and the interests, rights and freedoms of data subjects on the other side. Thus, Art. 6 (1) lit. f GDPR can be described as a "pacemaker" that provides for some flexibility within the otherwise rather static regime of the GDPR. However, according to the *CJEU's Grand Chamber* and in order to avoid an erosion of the requirements for valid consent, Art. 6 (1) lit. f GDPR needs to be interpreted restrictively, too.[71]

---

[69] Emphasis added.

[70] Emphasis added.

[71] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 93; see also: CJEU, Judgment of 24.2.2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, para. 73. For a more comprehensive justification hereof: *Sattler*, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 I GDPR,

Clearly, the EU legislator has failed to provide any – even abstract – criteria that might be employed by a User when balancing the interests between the data subjects' privacy and the interest of a User to access, use or share personal data as a crucial source for downstream innovation. The case law is far from providing precise guidelines as to the application of Art. 6 (1) lit. f GDPR, too. The *CJEU* has recently decided that the customers of an online network such as *Facebook* will not reasonably expect that the operator of the network will process customers' personal data for the purposes of personalised advertising, without his or her consent. Consequently, the interests and fundamental rights of a customer of *Facebook* override the interest of *Meta* in personalised advertising by which it funds its business model.[72] Therefore, multi-sided platforms such as "social networks" cannot rely on Art. 6 (1) lit. f GDPR when processing personal data as source for personalised advertising.

Consequently, Art. 6 (1) lit. f GDPR may provide a legal basis when personal data is processed in order to satisfy a User's right to access, use and share data according to Art. 4 and Art. 5 DA. However, if the User is identical to the data subject, such request can be construed as containing a consent by this User to such data processing.[73] In this case Art. 6 (1) lit. f GDPR would only be applicable insofar as the processed data relates to other data subjects (multi-relational data). Yet, the application of Art. 6 (1) lit. f GDPR will often be limited by the fact that the processing of *sensitive* personal data is beyond its scope.

c) Art. 4 and 5 DA as legal obligation or (substantial) public interest?

Once it is accepted that the reference to consent and contract in Rec. 34 s. 8 DA is only exemplary, it seems possible to assume that the access, use and sharing of

---

in: Lohsse/Schulze/Staudenmayer (eds.), Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V, 2020, p. 223 ss.; *Sattler*, Informationelle Privatautomomie, 2022, p. 278 ss., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

[72] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 117.

[73] *Wiebe*, Der Data Act – Innovation oder Illusion?, GRUR 2023, 1569 (1574); *Antoine*, Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht, CR 2024, 73 (74/para. 6).

personal data could also be based on Art. 6 (1) lit. c or lit. e GDPR and, where sensitive data is concerned, on Art. 9 (2) lit. g GDPR.

According to Art. 6 (1) lit. c GDPR processing shall be lawful insofar as it is necessary for compliance with *a legal obligation* to which the controller is subject. According to Art. 6 (1) lit. e GDPR processing shall be lawful insofar as it is necessary for the performance of a task carried out in the *public interest*. Art. 9 (2) lit. g GDPR allows the processing of sensitive personal data insofar as it is necessary for reasons of *substantial* public interest, on the basis of Union or Member State law.

In the context of the preparatory documents, the *EU-Commission's Proposal* of the DA and the *Council's Mandate*, it had already been argued that these legal bases should be applicable within the context of Art. 4 (1) and Art. 5 (1) DA.[74] Consequently, both norms could provide such legal obligations outside the GDPR or a (substantial) public interest which – in connection with the opening clauses in Art. 6 (1) lit. c, lit. e GDPR and Art. 9 (2) lit. g GDPR – would help to achieve the objective of the DA to improve data-driven downstream innovation. However, such an interpretation of Art. 4 (1) and Art. 5 (1) DA – at first sight – contradicts the wording of Art. 4 (12) and Art. 5 (7) DA. According to the latter, personal data is only to be made available by the Data Holder to a User, who is not the data subject, where there is a valid legal basis for processing "under Art. 6 GDPR". Thus, the wording of Art. 4 (12) and Art. 5 (7) DA, the wording of Rec. 34 DA and in particular the clear statement in Rec. 7 s. 7 and s. 9 DA that the DA "does not constitute a legal basis for the collection or generation of personal data by the data holder" nor "create a legal basis for providing access to personal data" speak against an interpretation according to which the opening clauses of the GDPR are completed by the DA in a manner that effectively culminate in Art. 4 (1) and Art. 5 (1) DA as constituting legal bases to process (sensitive) personal data.[75]

---

[74] *Specht-Riemenschneider*, Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, ZEuP 2023, 638 (665 ss.).

[75] Of the same opinion: *Antoine*, Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht, CR 2024, 73 (74/para. 7); *Czychowski*, Shaping the Data Economy: Ausgestaltung von Datenüberlassungsverträgen aus Herstellerperspektive, CR 2024, 80 (83/para. 17). With a different opinion, however, referring to a proposal of a Rec. 24 by the Councils's Mandate that was not successful in the Trilogue: *Specht-Riemenschneider*, Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, ZEuP 2023, 638 (667 s.). *Specht-Riemenschneider* limits the application of Art. 6

When all details of both norms are considered, an astonishing ambiguity occurs. Both norms refer to the GDPR for "any personal data" in a situation, in which "the user *is not* the data subject whose personal data is requested".[76] In an inverse effect Art. 4 (12) and Art. 5 (7) DA could be interpreted to allow a data holder to make personal data available to a User, who *is* the data subject, or to a third party of the User's choice, irrespectively of whether or not there is a valid legal basis for processing under the GDPR.

Indeed, such interpretation could be supported by the fact that Rec. 7 DA distinguishes between situations, in which the User is the data subject and situations, in which the User is not the data subject. According to Rec. 7 s. 8 DA only as far as the former is concerned "*this Regulation imposes an obligation* on data holders to make personal data available to users or third parties of a user's choice upon that user's request".[77] This statement seems to imply, that both, Art. 4 (1) and Art. 5 (1) DA, constitute such a legal obligation as required by Art. 6 (1) lit. c GDPR. However, any request to make data available by a User, who *is* identical with the data subject, already implicitly contains this User's consent. Therefore, Rec. 7 s. 8 DA and its imposing of an obligation on the Data Holder is – as far as personal data and the GDPR is concerned – redundant.

d) Art. 6 (1) lit. a and Art. 9 (2) lit. a GDPR: Consent as Synchroniser

Owing to the difficulties to reliably distinguish between personal and non-personal data, Data Holders are well advised to assume mixed data sets and to provide access to such data or share such data only if Users can provide a contract, that suffices the demands of Art. 14 (12) and (13) DA and Art. 6 (1) lit. b GDPR (contract) or if consent by all data subjects has been obtained (Art. 6 (1) lit. a GDPR). However, owing to the difficulties to reliably distinguish between personal and sensitive data, Data Holders are well advised to provide access to such data or share such data only if Users can provide a contract as regards the non-personal data and an explicit consent as regards the sensitive personal data.

---

(1) lit. c. and Art. 6 (3) GDPR to cases where a User is identical to the data subject and demands access to personal data according to Art. 4 (1) DA. Contrastingly, where a User is not the data subject but requests access to or the sharing of personal, Art. 6 (1) lit. c GDPR shall not apply.

[76] Emphasis added.

[77] Emphasis added.

Although such an approach seems to be a possible solution, this combination of contract (as regards non-personal data) and *explicit* consent (as regards sensitive personal data) needs to adhere to the complex requirements stipulated by Art. 8 and Art. 9 DA and by Art. 6 (1) lit. a, Art. 7 (3), (4) and Art. 9 (2) lit. a GDPR.[78]

2. Art. 6 (2) lit. b DA: No legal basis for the processing of personal data

Art. 6 (2) lit. b DA is the murkiest provision on the relationship of the DA and the GDPR. Art. 6 (1) DA stipulates that any third party that has received data pursuant to Art. 5 DA shall only process such data for the purposes and under the conditions agreed with the User and, insofar as personal data is concerned, subject to the laws on the protection of personal data. According to Art. 6 (2) lit b. DA the third party shall not "notwithstanding [Art. 22 (2) lit. a and lit. c GDPR] use the data it receives for profiling, unless it is necessary to provide the service requested by the *user*".[79]

At first glance it is astonishing that the request of a User – who is not identical to the data subject – seems to be sufficient to legitimise the processing of personal data for profiling. The corresponding recital hardly sheds any light on the objectives pursued with this provision. Rec. 39 s. 1 DA merely repeats that third parties should "refrain from using data falling within the scope of this Regulation to profile individuals unless such processing activities are *strictly necessary to provide the service* requested by the user".[80]

One could consider that Art. 6 (2) lit. b DA implicitly refers to Art. 6 (1) lit. b GDPR. However, the latter is only applicable in cases where the controller and the data subject have entered into a contract. It is not applicable in cases where the User has entered – or requested to enter – into a contract with a third party.[81] Moreover, the reference to Art. 22 (2) lit. a GDPR ("notwithstanding"), a provision which parallels Art. 6 (1) lit. b GDPR in case of profiling, would hardly

---

[78] See below Section B.III.

[79] Emphasis added.

[80] Emphasis added.

[81] Art. 6 DA seems to be applicable irrespectively of whether third party acts as controller (Art. 24 (1) GDPR) or merely as processor (Art. 28 (1) GDPR). However, if the third party undertakes the profiling in order to fulfil its own service obligations towards the User, the former will more likely be a controller or a joint controller (Art. 26 GDPR).

make sense if Art. 6 (2) lit. b DA was meant to have any scope of application, independently from Art. 22 GDPR.

Consequently, it is not convincing to interpret Art. 6 (2) lit. b DA as a legal basis for profiling outside the GDPR.[82] Indeed, any event in which a mere request by the User towards a third party for particular services could legitimise the profiling of a data subject would amount to a contract which is detrimental to the data subject.[83] Such a contract would be void, both, according to to Sec. 242 German Civil Code and according to the European principle of good faith.

This generally leaves room for two interpretations: *Firstly*, it could be a mistake that Art. 6 (2) lit. b DA refers to the User irrespectively of whether or not the User is identical with the data subject. It was not until the Trilogue that the tensions between the DA and the GDPR became adequately apparent. While such increased awareness led to the provisions in Art. 4 (12) DA and Art. 5 (7) DA which explicitly distinguish between Users, who are also data subjects and Users, who are not data subjects, such differentiation might have been overlooked in Art. 6 (2) lit. b DA. Thus, the latter could be read as if it contained the words "user, who is the data subject" instead of "user". Such an understanding would allow for an application of Art. 6 (1) lit. b GDPR or – more convincingly – would allow to interpret the request by the User, who is the data subject, for services based on a profiling to imply a consent (Art. 6 (1) lit. a GDPR) in such profiling.[84] However, such an interpretation which is contrary to the explicit

---

[82] Likewise, EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, 18.6.2021, p. 16s. para. 57-58; *Specht-Riemenschneider*, Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO, ZEuP 2023, 638 (664); Arguing in favour of such a legal basis outside of the GDPR, however based on the DA-Proposal: Position Paper of the German Bar Association on the Proposal for a Regulation on harmonised rules on fair access, July 2022, p. 17, available at https://anwaltverein.de/de/newsroom/sn-40-22-vorschlag-der-eu-kommission-fuer-ein-datengesetz (28.2.2024).

[83] Similarly, it is doubtful that a contract between a User, who is not identical with the data subject, and a third party can – as such – constitute a legitimate interest in favour of the User according to Art. 6 (1) lit. f GDPR. However, supporting such a solution: *Antoine*, Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht, CR 2024, 73 (75/para. 10).

[84] Likewise: *Hennemann/Steinrötter*, Der Data Act, NJW 2024, 1 (4/para. 15); similar for any request by a User who is identical to the data subject: *Wiebe*, Der Data Act – Innovation oder Illusion?, GRUR 2023, 1569 (1574); *Antoine*, Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht, CR 2024, 73 (74/para. 6).

wording seems superfluous as Art. 6 (2) lit. b DA already refers to both options, the necessity for the performance of a contract (Art. 22 (2) lit. a GDPR) and the consent by the data subject (Art. 22 (2) lit. c GDPR).

Alternatively, Art. 6 (2) lit. b DA could be understood as a provision that is merely concerned with the relationship between the third party and the User. Such interpretation is supported by the headline of Art. 6 DA ("Obligations of third parties receiving data at the request of the user") and by the fact, that Art. 6 (2) lit. b DA seems to avoid any material statement as regards the protection of personal data. According to such an interpretation a third party might use the personal data for profiling in order to provide a service requested by the User. However, the legality of such processing under the GDPR would still depend on whether such User and, therefore, the third party[85] are able to provide a legal basis for such profiling according to Art. 22 (2) GDPR. Consequently, it would be the objective of Art. 6 (2) lit. b DA to uphold the User-centric approach of the DA.[86] Third parties, who receive data via a User, who is not the data subject would be prohibited from any profiling, unless such profiling was legal under the GDPR *and* necessary to provide the services request by the User. Thus, Art. 6 (2) lit. b DA would merely constitute an additional requirement for the third party to always involve the User, who's relying on Art. 5 (1) DA has enabled the third party to process the respective personal data. As data subjects can still legitimise such profiling by third parties autonomously according to Art. 22 (2) lit. a and lit. c GDPR such a requirement to involve the User in case of Art. 5 (1) DA does not impair the rights assigned to the data subject under the GDPR. According to this interpretation Art. 6 (2) lit. b DA is, therefore, consistent with Art. 1 (5) s. 3 DA as it causes no conflict between DA and GDPR.

III. Complexity of consent management for multi-relational data

As has already been mentioned the tension between Art. 4 and Art. 5 DA and the GDPR results from the diametrical objectives of both Acts, the difficulties to distinguish between personal and non-personal data and the difficulties to

---

[85] In this case the third party would most likely be a processor according to Art. 28 (1) GDPR, whilst the user remains the controller according to Art. 24 (1) GDPR.

[86] See *Eckardt/Kerber*, Designing the Bundle of Rights on IoT Data: The EU Data Act, Section E (Chapter 1 in this volume); *Zech*, Data Access Rights as Property Rights, Section C (Chapter 4 in this volume); *Metzger*, Contracts under the Data Act: Review of standard terms and FRAND conditions, Section C (Chapter 5 in this volume).

distinguish between personal and sensitive personal data. Moreover, and as a consequence of the User-centric approach of the DA it is unlikely that third parties who require access to personal data for data-based innovation will approach any Users, who are identical with the data subjects. Such a time-consuming strategy typically raises prohibitive transaction costs. Instead, third parties will approach professional Users such as providers of IoT-devices or related services (for example operators of car leasing pools or car rental services), who – via Art. 4 (1) and Art. 5 (1) DA – can provide access to data generated by a multitude of connected products and related services. As such data sets potentially contain (sensitive) personal data of many data subjects, such professional Users and their Data Recipients should typically rely on an explicit consent by all data subjects.

It is beyond the scope of this article to analyse all challenges that such an explicit consent poses. Thus, it must suffice to emphasis three crucial issues.[87] Coping with these challenges is a necessary precondition to achieve the objectives of the DA as far as personal data is concerned.

1. Freely given consent

It is essential not to interpret Art. 4 (11) and Art. 7 (4) GDPR as a strict prohibition of bundling a contract and a consent.[88] According to the view expressed here and in agreement with the prevailing view in the private law literature, when assessing the voluntariness of consent pursuant to Art. 7 (4) GDPR, it is

---

[87] Additionally, it could be considered whether data subjects have the capacity to temporarily waive their right to withdraw a given consent at any time and without cause under Art. 7 (3) GDPR. Such a right would allow for more stable contractual relationships between data subjects and controllers in general and seems particularly crucial in order to facilitate the right to access and share personal data in real-time. Such an option to waive the right to withdraw consent seems imperative when data subjects act in exercise of their trade, business or profession. However, even data subjects who are consumers should – under additional safeguards – be able to temporarily waive their right to withdraw consent: *Sattler*, Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art. 6 I GDPR, in: Lohsse/Schulze/Staudenmayer (eds.), Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V, 2020, p. 225 (243 ss); *Sattler*, Informationelle Privatautonomie, 2022, p. 328–356., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

[88] *Sattler*, Informationelle Privatautonomie, 2022, p. 298–327 ss., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

only necessary to take all circumstances of the individual case into account when assessing whether or not the controller has made the fulfilment of a contract dependent on consent to data processing, even though this processing is not necessary for the fulfilment of the contract.[89] In other words, Art. 7 (4) GDPR reminds the controller *ex ante* and the data protection authorities and courts *ex post* to pay attention if controllers combine the conclusion of a contract and consent, even though the performance of the contract does not necessarily require such consent. This understanding can already be inferred from Rec. 43 s. 1 GDPR, which cites a situation in which there is a clear imbalance between the data subject and the controller as an example in which it is unlikely that the data subject has given such consent voluntarily.

As a result, Art. 7 (4) GDPR encourages data controllers to separate the contract from the consent and, if these declarations are linked, to scrutinise if this combination of contract and consent is potentially only accepted because the data subject finds itself – in the individual case – in a position of structural ("imbalance") or situational ("all circumstances") dependency. In this case the data subject's consent may no longer be accepted by law as a manifestation of autonomy.[90]

As regards a structural imbalance the *CJEU* held, that the requirements for valid consent "must be interpreted as meaning that the fact that the operator of an online network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able to validly consent." Instead, even in cases where the operator of such a network has a dominant market position, this fact is only "an important factor in determining whether the consent was in fact validly and, in particular, freely given".[91]

---

[89] *Sattler*, Informationelle Privatautonomie, 2022, p. 298 s., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

[90] With examples for such structural or situational inferiority: *Sattler*, Informationelle Privatautonomie, 2022, p. 298 s., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

[91] CJEU (Grand Chamber), Judgement of 4.7.2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, para. 154. Contrastingly, suggesting a stricter interpretation of Art. 7 (4) GDPR as regards a consent *vis-à-vis* gatekeepers (Art. 3 DMA): *Sattler*, Informationelle Privatautonomie, 2022, p. 311–316., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

While the specific obligations to be derived from Art. 7 (4) GDPR remain to be controversial, the provision at any rate serves to materialise the formal self-determination of the data subject in individual cases. Art. 7 (4) GDPR thus constitutes a central support for the informational autonomy of data subjects.

2. Informed consent

According to Art. 5 (1) lit. a GDPR data processing is only lawful if it is carried out in a transparent manner. Art. 4 No. 11 GDPR states that consent must be given in an informed manner. The requirement of informed consent is an objective of the GDPR and an obligation directed at the controller to provide information to the data subject before consent is given. However, being informed does not mean an actual mental status of the data subject at the time consent is given. As a result, a data subject should be considered to be informed once it had reasonable options to obtain knowledge about the essential characteristics of the data processing and was able to intellectually grasp their significance before giving consent. Being informed within the meaning of Art. 4 No. 11 GDPR, should, therefore, only mean a potential status of the average data subject. A status, however, that it can actually achieve with reasonable effort.[92]

Consequently, a data subject's lack of interest in easily accessible and factually correct information is at data subject's risk because the controller does not bear such risk of negligent behaviour by a data subject. While the data subject is generally responsible whether or not it actually takes note of the information that is accessible with reasonable effort, the controller bears the risk that the essential information is correct, transparent and complete in terms of content and is available in such a way that the data subjects can easily access and comprehend it if they wish to do so.[93]

---

[92] *Sattler*, Informationelle Privatautonomie, 2022, p. 219 ss., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

[93] In order to provide the controller with a certain degree of legal certainty, the most important information obligations are specified by the GDPR, although these are not exhaustive. This includes information on the identity of the controller, the purposes of the data processing (Recital 42), the category of data processed (Art. 9 (1) GDPR) and the types of processing, including their use for automated decision-making in accordance with Art. 22 (2) lit. c) GDPR or their transfer to third countries (Art. 49 (1) s. 1 lit. a GDPR). According to Art. 7 (3) s. 3 in

As the GDPR follows a risk-oriented approach,[94] the requirements for the provision of information depend on the risk of data processing for the rights of the data subject. This is important because the effect of information – as with medicine – depends largely on the dose (risk of information overload). As a result, there exists a dilemma between the comprehensibility and completeness of information.

Multi-levelled and modular consent forms may offer a solution to this dilemma.[95] While the first level enables an easy understanding of the main risks for the data subject, the granularity and complexity of the information is increased at the – still easily accessible – higher levels. Such a tiered model ensures that those data subjects can sufficiently inform themselves, who either have a high data protection preference or who are prepared to deal with complex information and base their decisions on it.

3. Consent for specific purposes

It is obvious that the objective to enable downstream innovation based on personal data can easily shipwreck on the rock of "purpose limitation". According to Art. 6 (1) lit. a GDPR the data subject must consent to the processing "for one or more specific purposes". As Art. 5 (1) lit. b GDPR stipulates, personal data collected for specified, explicit and legitimate purposes shall not be processed further in a manner that is incompatible with those purposes (principle of 'purpose limitation'). However, Art. 5 (1) lit. b GDPR clarifies that further processing for scientific research purposes shall "not be considered to be incompatible with the initial purposes".

Based on this exemption the German Medical Informatics Initiative has suggested a "Patient Consent Form Template" that comprises information and consent forms for patients and the use of – typically pseudonymized – health

---

conjunction with Art. 13 (2) lit. c GDPR, the controller must also inform the data subjects about the – regularly existing – right of withdrawal.

[94] See Art. 35 GDPR.

[95] Suggesting a combination of a unitary risk-based labelling similar to a nutrition label and a Privacy Control Cockpit: *Sattler*, Informationelle Privatautonomie, 2022, p. 363 ss. and 383 ss., available at https://www.mohrsiebeck.com/en/book/informationelle-privatautonomie-9783161619069?no_cache=1 (8.5.2024).

data for research purposes.[96] According to Art. 1 (2) of this template patient data can be made available to companies conducting medical research for the predetermined scientific research purpose. Additionally, such use of health data requires prior review and approval by an independent ethics committee.

While it is not possible to analyse and evaluate this proposal within this publication, the template provides an insight that innovation based on (sensitive) personal data is – by the definition of innovation – an open-ended concept. Thus, it is essential to find solutions which leave some legroom for a dynamic adjustment of purposes that does not require a re-assessment by each data subject or – if such re-assessment is considered necessary – can be obtained via technically feasible means, such as PIMS.

C. Conclusions

It has two crucial benefits that the scope of the DA includes personal data. *Firstly*, the DA enables a reform of Art. 15 and Art. 20 GDPR and thus strengthens the rights of data subjects. *Secondly*, the DA reinforces the second objective of the GDPR, namely the enabling of a free movement of personal data within the Union, Art. 1 (3) GDPR.

However, the acknowledgment of personal data and even sensitive personal data as a resource of data-driven innovation requires a comprehensive synchronisation of DA and GDPR. Otherwise, the User's right to access, use and share data will run idle. If natural persons use connected products and related services, personal data is regularly generated. The (real) behaviour of the data subjects also determines whether particularly sensitive personal data is generated. Consequently, the controller (Data Holder/User/Data Recipient) must – by default – assume that data sets contain such sensitive data. However, as the DA does not modify the GDPR with regard to the legal bases to process (sensitive) personal data, the interpretation and application of the GDPR will be decisive for the success of the DA.

---

[96] Medical Informatics Initiative, Consent Working Group, Patient Consent Form Template, version 1.6d of 16.4.2020, English translation of 10.11.2020, available at https://www.medizininformatik-initiative.de/en/template-text-patient-consent-forms (8.5.2024).

As analysed above the burden of synchronising Art. 4 and Art. 5 DA and the GDPR lies on consent. As this will require a complex cascade of consents by a multitude of data subjects, such synchronisation depends on the development and implementation of efficient and effective consent management systems, such as PIMS.

Part IV

Challenge 2: The Interfaces with Copyright Law

Chapter 8

»Without prejudice«: The Interface of the Data Act and Copyright

Benjamin Raue*

A. Introduction

The aim of the Data Act is to "remove barriers to a well-functioning internal market for data" (recital 4). It contributes to this aim by attributing a transferable right of data access to users (Art. 3-5 Data Act).

But that right is of little use as far as its exercise is hindered or made uncertain by other data regulations. A lot has been said and written about the collision of the data act access right with data protection rules and the protection of trade secrets: You can find two contributions about this in this volume by Andreas Sattler[1] and by Tanya Aplin[2].

In my contribution I will explore the interface between the data access right and copyright, which has not gained much attention so far. This is because the overlap between the data regulated by the Data Act and copyright is not as far reaching as that with data protection and trade secrets. But it still exists as this paper will show in part II. Part III. explores the relationship between the Data Act and the meaning of the "no prejudice" clause in Art. 1(8) of the Data Act. This paper will show that the Data Act is not intended to establish an external exception to copyright. Part IV. analyses three categories of copyright protected data that have been addressed separately by the Data Act and are excluded from

* Prof. Dr. Benjamin Raue, Professor of Private Law, Law of the Information Society and Intellectual Property Law at University of Trier, Germany.

[1] About the interface with data protection, *Sattler*, Data Act and Data Protection Law (Chapter 7 in this volume).

[2] About the interface with trade secrets, *Aplin*, The Data Act and trade secrets: an experiment in compulsory licensing (Chapter 6 in this volume).

certain data access rights. Part V. shows ways to access, transfer and use copyright protected data on the basis of exceptions and limitations of copyright.

B. The overlap with copyright

A paradigm of copyright is that (semantic) information as such is not protected by copyright law – and therefore raw data is in the public domain from a copyright perspective.[3] A work is only protected under Art. 2 of the InfoSoc Directive if it qualifies as "its author's own intellectual creation".[4] It requires "creative abilities"[5] which excludes machine generated data from copyright protection as a work.

However, 'data' as defined in Art. 1(1) of the Data Act includes data in form of "sound, visual or audio-visual recording". Unfortunately (from the perspective of data access and use), the copyright free semantic information may be encapsulated in a copyright protected shell, such as a photograph or a video, a phonogram or a database[6] which can all be protected by a neighbouring copyright. In that case, the stored semantic information is still free, but (technical) actions necessary to access or process that information may still infringe copyright. Furthermore, the copyrightability of data might be an indicator that this data is not covered by the Data Act (see below IV.).

---

[3] See for example *Zech*, Information als Schutzgegenstand, 2012, p. 37 ff., 54 ff., 123 f., 246 ff.; *Hofmann*, Zehn Thesen zu Künstlicher Intelligenz (KI) und Urheberrecht, WRP 2024, 11 (marginal no. 23); *Raue*, Rechtssicherheit für datengestützte Forschung, ZUM 2019, 684 (686).

[4] See only CJEU, Judgement of 16.7.2009, Infopaq International A/S/Danske Dagblades Forening, C-5/08, ECLI:EU:C:2009:465, para. 37.

[5] CJEU, Judgement of 7.3.2013, Eva-Maria Painer/Standard VerlagsGmbH, C-145/10, ECLI:EU:C:2013:138, para. 89.

[6] This particular overlap between copyright and data access is analysed in detail by *Wiebe*, The Database Right and Art. 43 of the Data Act (Chapter 9 in this volume); *Leistner*, Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, 2017, p. 27.

I. Sound recordings

Sound recordings can be protected by the neighbouring right of a phonogram (Art. 2(c) InfoSoc Directive; see for example sec. 85 German Copyright Act (UrhG)).

II. Visual or audio-visual recording

1. Photographs

Photographs may be protected by the photographer's neighbouring right. This right is not harmonised in the EU. The requirements and the scope of protection are therefore determined by Member State law. In Germany and Austria, the copyright protection does not require originality in the sense of a copyright protected work but does require a minimum amount of personal intellectual effort or a human act of creation.[7] This requirement is usually not met when a machine automatically records pictures, such as a camera installed in a car. However, in a somewhat far-fetched decision, the Austrian Supreme Court (OGH) has granted copyright protection to weather cam images because they were set up in a certain angle by a human and the operator has the authority to determine the subject to be recorded and the time at which it is recorded by operating the system.[8] Therefore, it is not safe to exclude, for example, satellite, door bell or security camera pictures per se from copyright law protection.

2. Film recordings

Film producers are awarded a neighbouring right for the first fixation of a film (Art. 2(d) InfoSoc Directive). Object of that fixation needs to be a film work which requires human originality. Automated machine recordings are not covered by that right. However, at least under German copyright law (sec. 95 German Copyright Act (UrhG)), there is a neighbouring right for all "moving pictures" even if they do not constitute a film work. The German Federal Court of Justice (BGH) has not decided whether moving picture require a minimum

---

[7] BGH, Judgement of 8.11.1989 – I ZR 14/88, GRUR 1990, 669 (673) – Bibelreproduktion; BGH, Judgement of 7.12.2000 – I ZR 146/98, GRUR 2001, 755 (757) – Telefonkarte; OGH, Judgement of 1.2.2000 – 4 Ob 15/00k, ZUM-RD 2001, 224 (228); *Schulze/Dreier*, in: Dreier/Schulze (eds.), Urheberrechtsgesetz, 8th Ed. 2024, § 72 marginal no. 7.

[8] OGH, Judgement of 1.2.2000 – 4 Ob 15/00k, ZUM-RD 2001, 224 (228).

amount of personal intellectual contribution or organisational efforts, but this is assumed to be the case in literature.[9] However, even in this case, copyright protection may be awarded by courts if the setting of the recording has been influenced by a human being.

Therefore, it is not safe to exclude, for example, satellite, doorbell or security camera recordings per se from copyright protection.

III. Sensor Data

Sensor data such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed (recital 15 Data Act) can only be protected by copyright against extraction and/or reutilization if they are contained in a sui-generis database according to Art. 7 Database Directive. This particular overlap between copyright and data access and the scope of Art. 43 of the Data Act is analysed in detail by Andreas Wiebe (see Chapter 9).[10]

IV. Acts covered by copyright

Accessing, transferring and processing copyrighted data may infringe the right of reproduction (Art. 2 InfoSoc Directive) and the right of communication to the public (Art. 3 InfoSoc Directive). The reproduction right is the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproductions by any means and in any form, in whole or in part. This means even temporary reproductions of copyright protected material, for example in the RAM of a computer, is covered by the reproduction right. If copyright protected data is made accessible to the public, then the act is covered by the right of communication to the public.

The question of whether the extraction and re-utilization of sensor data from a sui generis database infringes the right conferred by Art. 7 of the Database Directive has been subject to discussion by other scholars before.[11]

---

[9] See for example *Manegold/Czernik*, in: Wandkte/Bullinger (eds.), Urheberrecht, 6th edition 2022, UrhG, § 95 marginal no. 1.

[10] See also *Kim*, Der Datenbankschutz sui generis nach dem Data Act, MMR 2024, 87.

[11] *Leistner*, Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform, in: Lohsse/Schulze/Staudenmayer (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, 2017, p. 27.

C. No prejudice to copyright

The Data Act remains largely passive with regard to this overlap with copyright law and merely states in Art. 1(8) that the Data Act is "without prejudice" vis-à-vis EU and Member State legal acts protecting intellectual property rights. It clarifies in recital 30 that data may be used and transferred to third parties for any lawful purpose – but that any intellectual property rights "should be respected" when handling the data. The evaluation obligation of the Commission in Art. 49(1)(e) of the Data Act shows that the Data Act should not negatively affect intellectual property rights including copyright. The Commission will have to demonstrate the "absence of any impact on intellectual property rights". Therefore, it is safe to assume that the Data Act is not intended to establish an external exception to copyright law.

This means that data which is protected by copyright law can only be accessed, transferred and used to the extent that a copyright exception allows those acts (see part E. below) or that they are authorised by the copyright holder.

D. Special category of data mentioned by Data Act provisions

I. User recorded, transmitted, displayed or played content

According to recital 16 of the Data Act, product data (Art. 2(16) Data Act) covers mainly data collected by sensors embedded in products. Not covered by the Data Act are unrelated software and content such as textual, audio or audiovisual content which the "user records, transmits, displays or plays, as well as the content itself" as it is "often covered by intellectual property rights". The exception also applies to content that is merely stored or processed on the devices. It is still to be determined whether that exception applies to content that is automatically recorded by the device, for example by a doorbell camera. The active wording ("the user records") and the aim of the Act to regulate sensor data seems to indicate that only active recording decisions by users trigger the copyright exception.

II. Exportable data protected by intellectual property rights of the provider of data processing services or a third party

The Data Act aims to facilitate the switching of services and the related customer's exit strategy (recital 82). Still, the exportable data does not include "any assets or data protected by intellectual property rights [...] of providers of data processing services or third parties" (Art. 2(38), recital 82 Data Act).

III. Copyright protected data of the user

The Data Act further mentions in Art. 13(5)(b) data protected by intellectual property rights of the other contracting party. As this provision only concerns contractual terms unilaterally imposed by another enterprise, it is outside the scope of this paper.

E. Enabling data processing through copyright exceptions

There are mainly two copyright exceptions that allow the processing of copyright protected data: the exception for temporary reproductions (Art. 5(1) InfoSoc Directive) and the exception for text and data mining (Art. 4 CDSMD). The processing of data for non-commercial scientific research may also be permitted under Art. 3 of the CDSM Directive and for private use under Art. 5(2)(b) of the InfoSoc Directive, which will not be examined here due to the limited personal scope of the exceptions.

I. Temporary reproductions (Art. 5 (1) InfoSoc-Directive)

Art. 5(1) of the InfoSoc Directive allows temporary acts of reproduction if three further conditions are met. First, they need to be transient and form an integral and essential part of a technological process. That excludes reproductions that are not automatically deleted after the analysis.

Second, their sole purpose must be to enable a lawful use. Here, recital 9 of the CDSM Directive is of help as it clarifies that temporary reproductions necessary for text and data mining are covered by the exception as the exception "should continue to apply to text and data mining techniques that do not involve the making of copies beyond the scope of that exception".

Third, the reproductions must have "no independent economic significance". According to the case law of the CJEU, this does not refer to the lawful temporary use as such but only to advantages that must be "either distinct or separable from the economic advantage derived from the lawful use of the work concerned and it must not generate an additional economic advantage going beyond that derived from that use of the protected work".[12] That means that the economic gain of the text and data mining analysis cannot be included in the economic analysis but only a further, separable use of the temporary reproductions themselves.

However, there is a fourth restriction for text and data mining in the case of the CJEU. The temporary reproductions must not alter the processed subject matter "as it exists when the technological process concerned is initiated", because the Court then deems those acts to "no longer aim to facilitate its use, but the use of a different subject matter".[13] However, it is unclear whether that only excludes alterations of those parts and in ways that affect the originality of the works – or whether that also includes technical changes to the data, for example to the file format.

As a final restriction, the exceptions based on Art. 5(1) of the InfoSoc Directive do not apply to sui-generis databases.[14]

In conclusion, data analysis based on Art. 5(1) of the InfoSoc Directive does not allow the modification of the temporarily reproduced data, the permanent storage of that data in order to create a permanent corpus, and it does not apply to sui-generis databases.

II. Text and Data Mining (Art. 3, 4 CDSM Directive)

Copyright exceptions aimed at processing data stored in a copyright shell are the two text and data mining exceptions in Art. 3 and 4 of the CDSM Directive. As the exception in Art. 3 of the CDSM Directive only covers reproductions for the purpose of scientific non-commercial analysis, this paper focuses on the

---

[12] CJEU, Judgement of 17.1.2012, Infopaq International, C-302/10, ECLI:EU:C:2012:16, para. 50.

[13] CJEU, Judgement of 17.1.2012, Infopaq International, C-302/10, ECLI:EU:C:2012:16, para. 53.

[14] Cf. *Dreier*, in: Dreier/Schulze (eds.), Urheberrechtsgesetz, 8th Ed. 2024, § 87c marginal no. 1.

broader exception of Art. 4 of the CDSM Directive, which also covers commercial text and data mining. In contrast to Art. 5 InfoSoc Directive, Art. 4 exempts the use of data contained in a sui generis database (Art. 4(1) CDSMD).

According to the legal definition in Art. 2(2) of the CDSM Directive, text and data mining is any "automated analysis of texts and data in digital form". Recital 8 shows that the definition covers all information available in digital form, regardless of its categorical classification, in particular "sounds, images or [other] data" in addition to text. Therefore, data covered by the Data Act are also covered by the text and data mining exception of the CDSM Directive.

Art. 4 of the CDSM Directive exempts from copyright all reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining. However, Art. 4(2) of the CDSM Directive imposes a time limit on reproductions and extractions made pursuant to the exception covered by Art. 4(1) of the CDSM Directive. They may only be retained for as long as is necessary for the purposes of text and data mining.

The main shortcoming of data analysis covered by Art. 4(1) of the CDSM Directive is that, according to paragraph (3), it only applies on the condition that the use of the copyright protected data has not been "expressly reserved by their rightholders in an appropriate manner". Therefore, the copyright holders may restrict the automated analysis of data which is contained in a copyrighted shell. This may result in smaller datasets of lower quality and weaken the purpose of the data access right under the Data Act.

F. Conclusion

Data which are covered by the data access right of the Data Act might be protected by copyright, especially if they consist of photographs, film or audio recordings. It is unclear who is owner of those (neighbouring) copyrights. If the data holder or a third party is copyright holder (or claims to be), then there is a legal uncertainty whether the data storing and processing infringes copyright. If the user is not the copyright owner, then legal certainty only exists if the use is exempted from copyright by the copyright exceptions based on Art. 4 of the CDSM Directive. However, copyright owner may exercise their right to reserve the automated analysis of the copyrighted subject matter under Art. 4(3) of the CDSM Directive. In its evaluation of the Data Act (Art. 49), the Commission

should reflect whether to abolish the right to exercise a reservation under Art. 4(3) of the CDSM Directive to the automated analysis of data which falls under the data access right of the Data Act if that reservation is regularly made by the (alleged) right holders.

Chapter 9

The Database Right and Art. 43 of the Data Act

Andreas Wiebe*

The EU Data Act went into force on Jan. 11, 2024 and will be applicable from Sep 12, 2025.[1] Its main purpose is to promote the making available of data on the market in the interest of innovation by creating opportunities for developing new products and services. While in 2017 creation of a new exclusive right on data was contemplated,[2] it was soon realised that data with its special characteristics does not lend itself easily to concepts of exclusive rights in light of its design and consequences.[3] The focus shifted to establishing access rights to break up the factual exclusive control of data holders to tackle the problem of insufficient availability of data.

While no special intellectual property regime exists for data and protection under general civil law would be deficient and systematically flawed, the systems closest to protection of non-personal data are the database sui generis right and trade secret protection. Hence, a possible conflict arises between the access approach of the Data Act and the indirect protection of data under the Database

* Prof. Dr. Andreas Wiebe, Professor of Civil Law, IO and Competition Law, Media and Information Law, University of Göttingen, Germany, Andreas.Wiebe@jura.uni-goettingen.de.

[1] Regulation (EU) 2023/2854 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 2023/2854, 22.12.2023, p. 1-71.

[2] See European Commission, Building a European Data Economy (Communication), 10.1.2017, COM(2017) 9 final.

[3] *Wiebe*, Protection of industrial data – a new property right for the digital economy?, GRUR Int. 2016, 877; *Drexl*, Designing Competitive Markets for Industrial Data, JIPITEC 2017, 257 (272 et seqq).

Directive 1996/9/EC.[4] The legislator tried to solve this by providing an exclusionary provision in Art. 43 of the Data Act.

A. Art. 43 Data Act and its scope

I. The wording of Art. 43 DA

Art. 43 Data Act reads:

"The sui generis right provided for in Article 7 of Directive 96/9/EC shall not apply when data is obtained from or generated by a connected product or related service falling within the scope of this Regulation, in particular in relation to Articles 4 and 5 thereof."

Rec. 112 states the prevention of hindering the exercise of access rights through enforcement of the sui generis database right as the objective of the provision. The wording still is subject to interpretation. To understand the nature of the conflict between protection of databases and access rights to data under the DA, and to construct the proper scope of the provision, the broader picture of the background has to be viewed.

II. The concept of MGD and the scope of the DA

Art. 1 DA limits the application to product data and related services data. Art. 2(15) DA defines product data as "data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer".[5] Hence, the DA aims at IoT-generated data. These are a part of the concept of machine-generated-data (MGD) that is often used in the legal discussion as a counterpart to personal data. However, this antagonism exists only from a legal perspective as data protection law, esp. the GDPR, creates special legal rules for personal

[4] See also *Wiebe*, The Data Act Proposal – Access rights at the Intersection with Database Rights and Trade Secret Protection, GRUR 2023, 227.

[5] Art. 2(16) DA: 'related service data' means data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider.

data whereas MGD as raw data are subject to general rules in civil law and intellectual property law. However, MGD or raw data may also be regarded as personal data and then be subject to data protection rules.

MGD can be defined:

"as data recorded, collected, or generated independent of direct and economically significant human intervention by:

- sensors processing information received from equipment, software or machinery, whether virtual or real
- computer processes, applications or services.
- Sensor-generated data in IoT environment would include:
- data generated by sensors about the sensor and machine itself, e.g. data on machine performance;
- data generated/observed by sensors observing the environment in which sensors and machines operate, e.g. information on the soil recorded by sensors in smart tractors;
- the data resulted from the aggregations and processing of the two types of data above'."[6]

While this definition was not intended to be used as statutory definition, it clarifies the types of data included and the function of sensors. It also clarifies that the definition may include some pre-processing activities that are done directly by the sensor, such as data compression, data encoding, or transmission of raw data directly to the cloud structure. Data already structured in data warehouses and ready to be used for deriving insights should not be included in the definition of MGD.

The Data Act limits its scope in Art. 1 to data generated by the use of a product or related service. This delimitation seems to aim at MGD. While raw data even if produced by machines are immediately refurbished or in other ways formatted or processed by machines or sensors or just collected and categorised, this "curation" or formatting can hardly be separated from the generation process.[7] Recital 15 clarifies that this data is included in the scope of the DA.

However, Recital 15 also excludes derived and aggregated data from the scope that were included in the broader definition stipulated above. This may

---

[6] *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p. 32 et seqq.

[7] *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022.

not only lead to frictions as the scope of other sector-specific access rights is not limited in such a way, e.g., in the automotive sector pertaining to repair and maintenance information.[8] The inclusion of derived and aggregated data in the scope of legislation also is essential for innovation on secondary markets and hence necessary to achieve the objectives of the Data Act.[9]

III. MGD and the Database Right

The Database Directive had been subject to two evaluations in 2005 and 2018.[10] The results were rather critical on the design and effectiveness especially with respect to the sui generis right and suggested that the Database Directive provided an "outdated legal framework".

In the context of the Data Act another review of the Database Directive 96/9/EC was to be undertaken[11] to make it fitter for the needs of the data economy and provide for more legal clarity to improve access to and usage of data and databases with respect to machine generated data. Data and databases are used as input for various products or services. Legal protection and factual control may prevent aggregation and thus lead to market failure, lock-in effects and monopolistic markets. So, the objective was to bring legal clarity and promote access to data.

---

[8] See Regulation (EU) 2018/858 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, 14.6.2018, p. 1-218, Art. 61.

[9] See also *Podszun/Pfeifer*, Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, GRUR 2022, 953, 961.

[10] European Commission, First evaluation of Directive 96/9/EC on the legal protection of databases, 2005; European Commission/JIIP/Technopolis, Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, EU Publications, 16.5.2018; *Podszun/Pfeifer*, Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, GRUR 2022, 953.

[11] European Commission, Inception Impact Assessment EU Data Act, 28.05.2021, Ref. Ares(2021)3527151, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases_en (3.5.2024).

1. The uncertain scope of database rights as to MGD

One of the shortcomings of the Database Directive is its vagueness as to subject matter and scope. The CJEU tried to bring more clarity and issued four key decisions in 2004, establishing the distinction between generation of data and collection of data.[12] The Court narrowly interpreted the Directive to only consider investments separately shown as relating to the collection of data while excluding investments into the generation of data. While often MGD were considered to be excluded from protection because these data should be regarded as "generated", Leistner presented a differentiated view distinguishing between sensored data that could be observed by any third party and data generated by machines that are to be considered as having been generated.[13] This would roughly correspond to the distinction between data sensored by the machine itself and those sensored from the environment.

However, considerable uncertainties remained in the application of the dabase right to MGD. The CJEU decisions could be interpreted as indirectly resulting in excluding MGD from the scope of the database right since it could be argued that most investments of MGD producers go into the "creation" of this data.[14] Drawing a distinction between sensored data and machine-generated data becomes questionable in light of the fact that sensors are used for both scenarios – the gathering and creating of data. In the often cited "Autobahnmaut" case, the German Supreme Court considered registering lorry data at terminals by Toll Collect as being directed at data that pre-existed and constituting collection of data although you could make an argument in this case that the data was generated at the terminals.[15] Data generated by sensors and the processing and

---

[12] CJEU (Grand Chamber), Judgement of 9.11.2004, The British Horseracing Board and Others, C-203/02, ECLI:EU:C:2004:695; Judgement of 9.11.2004, Fixtures Marketing, C-46/02, ECLI:EU:C:2004:694; Judgement of 9.11.2004, Fixtures Marketing, C-338/02, ECLI:EU:C:2004:696; Judgement of 9.11.2004, Fixtures Marketing, C-444/02, ECLI:EU:C:2004:697.

[13] *Leistner*, The protection of databases, in: Derclaye (ed.), Research handbook on the future of EU copyright, Edward Elgar 2009, p. 427 (438).

[14] European Commission/JIIP/Technopolis, Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, EU Publications, 16.5.2018, p.20.

[15] German Supreme Court (BGH), Judgement of 25.3.2010 - I ZR 47/08, GRUR 2010, 1004 – Autobahnmaut.

aggregation of this data is hardly separable and renders drawing a distinction between generation and collection practically not feasible.[16]

2. Options for legislative solutions

To avoid these uncertainties and promote access and usage of data, the EU Commission considered the best option to be to exclude MGD completely from the database right. Alternative options were considered in directly excluding investments in generation of data by introducing a legislative assumption that MGD is "generated" and not "collected", or a rebuttable presumption that MGD databases do not require a substantial investment.[17] As a variation, qualitative aspects of data processing could be targeted and relevant investments limited to certain value-added forms of processing, including annotating the data, reformatting, curation of "historic" data (as opposed to real-time data streams), cleansing the data if done in direct connection with inserting the data into the database.

Another option was to specify a minimum requirement of substantial investment that will be hard to overcome by MGD. However, the consequence would be that this would favour big databases which in most cases are those containing MGD. As an innovative solution to this problem, it was suggested to refer to the average investment per data element.[18] As MGD are relatively cheap to produce and mostly contained in big databases, these would very often not qualify for protection and hence the goal would be achieved. The criterion could have been operationalised by requiring the database holder to show what the overhead costs are in the production of the database and over how many elements these costs can be spread.[19]

If the legislator had not acted, an issue could have arisen whether the Data Act would be lex specialis and access rights would have preference over the da-

---

[16] See *Sattler*, Schutz von maschinengenerierten Daten, in: Sassenberg/Faber (eds.), Rechtshandbuch Industrie 4.0 und Internet of Things, 2nd ed. 2020, p. 35 (48).

[17] See *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p. 59 et seqq.

[18] See *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p .62 et seq.

[19] See *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p .62.

tabase right. However, not any conflict would automatically trigger the lex specialis rule. Looking at previous access rights, e.g., Art. 1(2) Open Data Directive shows that IP rights can exclude the application of access rights at least to the extent that they are in concrete conflict. Drawing an analogy would not have been completely unjustified. Hence, in order to exclude a conflict between the database right and the access rights of the DA, the legislator had to act.

3. Interpretation of Art. 43 DA

Going back to the clause of Art. 43 DA, it is obvious that the legislator chose a minimalist approach that does not provide complete clarity, however. The aim is to exclude the database right for MGD. Hence, the most likely understanding would consider the provision to be an exception from the scope of protection of the database right with respect to databases containing data covered by the Data Act.[20] However, it could also be read as a confirmation that machine generated data (MGD) do not fulfill the substantial investment criteria.[21]

An alternative interpretation would imply that the database right should not be exercised only in cases of concrete conflict with the access rights established by the Data Act, esp. under Art. 4 and 5.[22] This would leave the rightholder in a position to enforce the database right against any other misappropriation activity outside the range of the access rights. But in this case explicit exception for the access rights could have been included in the Database Directive. Moreover, in light of the changes made to the clause in the course of the legislative process, the first interpretation should be favored.

---

[20] See also *Metzger/Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42.

[21] See *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by European Parliament's Committee on Legal Affairs (JURI), Brussels, 2022, p. 120.

[22] See *Drexl* et al., 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), Max Planck Institute for Innovation and Competition Research Paper No 22-05, 2022, para. 256 et seqq., considering an earlier version of the clause as an expression of the lex specialis character of the Data Act.

4. Remaining problems from Art. 43 DA

a) Treatment of "mixed databases"

Art. 43 DA does not give hints as how to treat mixed databases that contain MGD and other types of data and seem to be increasingly common.[23] To illustrate the problem with the example of "connected cars", in-vehicle access to data is mostly directed at MGD produced in the car, whereas "off-vehicle" access leads to a mixture and aggregation of MGD and other types of data. How then to identify and separate MGD so as not to include the pertinent investments into the establishment of protection?

From the wording of Art. 43 DA any database containing MGD seems to be covered. Such a broad construction may avoid the problems of identification and separation. But practically, it would mean excluding protection if already one dataset contains MGD.[24] This calls for a more practical solution. In the 2019 Guidance for the free flow of non-personal data in the EU concerning the mixture of personal and non-personal data, a requirement was introduced that database protection would be excluded if MGD and other data were "inextricably linked".[25] However, this could give rise to new problems of delineation. Another option would be to establish a rebuttable presumption according to which mixed databases are excluded from protection, unless the database holder can show that the database mostly consists of non-MGD.[26] Alternatively to 50%, a lesser threshold could be included as well.

---

[23] See *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p. 67.

[24] Favouring such broad exclusion *Drexl* et al., 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), Max Planck Institute for Innovation and Competition Research Paper No 22-05, 2022, p. 94 para. 261.

[25] European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (Communication), 29.5.2019, COM(2019) 250 final, p. 9.

[26] See also *Metzger/Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42, favouring limiting the exclusion to databases including "predominantly" MGD; *Drexl* et al., 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

b) Exclusion of aggregated data

The exclusion of aggregated/derived data from the scope of application of the Data Act, as laid down in recital 15, points to the difficulty of separating generated data from aggregated and derived data. This could result in database protection of MGD in aggregated form and have chilling effects on access rights established by the DA.[27] Other sector specific access rights are not limited in this way, e.g., in the automotive sector pertaining to repair and maintenance information.[28] This suggests that it would have been preferable to extend the application of the Data Act to aggregated and derived data as well, and exclude the application of the database rights with respect to this data included in a database accordingly.

B. Alternative instruments for protection of MGD

With the access rights approach being implemented in legislation, the discussion about the need for new exclusive rights on data got out of sight. While it might be argued that the Data Act establishes some kind of exclusive rights in the hands of the user who is the beneficiary of the access rights and is vested with control over access and use of data, his or her position is not comparable to holding an exclusive right in the intellectual property sense with full exclusive rights against third parties.

An interesting sideline in the discussion during the legislative process for the Data Act was the proposal to supplement the exclusion of MGD with a defensive right providing limited control inspired by protection of trade secret protection as laid down in the Accompanying Study.[29] Drawing on a scheme intro-

---

harmonised rules on fair access to and use of data (Data Act), Max Planck Institute for Innovation and Competition Research Paper No 22-05, 2022, p. 91 para. 255.

[27] See *Drexl* et al., 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), Max Planck Institute for Innovation and Competition Research Paper No 22-05, 2022, p. 10 para. 20 et seqq.

[28] See Art. 61 Regulation (EU) 2018/858.

[29] *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p. 71 et seqq. A related concept for protecting "shared data

duced in Japan, the basic idea was to declare the obtaining, the use and transmission of data from a specific database unlawful if the person knows or should have known at the time of obtaining, use or transmission that the person from whom they obtained the data was wrongfully using or forwarding the data. A similar concept was included in a draft of Art. 34 of the ALI-ELI Principles for a Data Economy[30] (and included in a Report of the German Commission on Data Ethics in 2019)[31]. Wrongfulness of use as the key notion would mostly draw on contractual prohibitions but could also include other illegal activities like hacking. An overall weighing of interests would be included. Certain types of permission could be included as was done with the permission of reverse engineering as well as reference to free speech in the Trade Secret Directive.

With this "defensive right" concept a middle ground between exclusive rights and unfair competition would be entered similar to trade secret law but not dependant on secrecy. While this concept would be based on a contractual approach and provide some flexibility, it would turn to a case-by-case analysis and result in some uncertainty. Protection along the value chain would be more burdensome and to be complemented by contractual arrangements. Most importantly, introducing an additional layer of protection only for MGD databases would enhance the complexity of the protection, enhance problems of delineation and hence and was not further followed on. Still, it can serve as an interesting intermediary solution for future discussion.

C. Suggestions not implemented with the Data Act

With two previous evaluations of the Database Directive having brought along no changes, there were high hopes put into the review associated with the enactment of the Data Act.[32] However, these were again disappointed. Much of the

---

with limited access" was introduced in Japan Unfair Competition Prevention Act (Act No 47 of 1993, revised in 2018) (UCPA); in Japan there is no sui generis protection of databases.

[30] See ALI/ELI Principles for a Data Economy, Data Transactions and Data Rights, As Adopted and Promulgated by The American Law Institute on May 18, 2021 and The European Law Institute on September 1, 2021.

[31] See Datenethikkommission, Gutachten der Datenethikkommission, 2019, p. 144.

[32] See *Derclaye/Husovec*, Sui Generis Database Protection 2.0: Judicial and Legislative Reforms, 11 LSE Law, Society and Economy Working Papers 15 (8 et seqq.), 2022, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=4138436 (3.5.2024); *Leistner/Antoine*, IPR and

strong criticism on the design of the database right present from the outset was brought up again without being sincerely considered by the Commission.

I. Term of protection

The term of protection of the database right is generally considered to be too long. Updating of databases initiates a new term and uncertainties connected with that may lead to "eternal" protection. A shorter term and a solution to the issue of different terms applying to different datasets is strongly needed. An interesting proposal was recently made to limit the term of protection to ten years beginning with the generation of the database, and to limit the prolongation of the term to one year only to be triggered by substantial changes but applying to the entire contents of the database.[33]

II. Public bodies as rightholders

One of the most burning issues relates to vesting database rights in public bodies. It has been long criticised that public bodies are not explicitly exempted from holding database rights, which led to diverging decisions in the Member States as to the application of the general copyright exemption of public works to the database right. While the European Commission thinks that the Open Data legislation had settled the issue, the respective provisions in the Public Sector Information (PSI) or Open Data legislation[34] leave ownership of the database right by public bodies untouched. This may lead to some unwanted effects. To avoid any disputes on the scope of the ODD, the complete exclusion of public bodies from being right holders would provide a clear and certain solution.[35]

---

the use of open data and data sharing initiatives by public and private actors, Study requested by European Parliament's Committee on Legal Affairs (JURI), Brussels, 2022, p. 49 et seqq.

[33] *Zier*, Investitionsschutz für Maschinendaten, 2022, p. 261 et seqq.

[34] Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information, OJ L 345, 31.12.2003, p. 90-96; Directive 2013/37/EU of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, OJ L 175, 27.6.2013, p. 1-8; Directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56-83.

[35] See also *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p. 85 et seqq.

III. Limitations and exceptions

While Art. 9 Database Directive established special limitations for the database right, suggestions have been made to adopt the general copyright limitations to the database right as well to provide for alignment.[36] Considering its character as a neighbouring right, this would not be unusual. Art. 3(1) and 4(1) of the DSM Directive 2019/790 on limitations for text and data mining followed this path already and alleviated many concerns of the research community. To extend this approach to many or all copyright exceptions could have the advantage of more systematic clarity and coherence. However, not all limitations appear to be useful in the database context. The example of private copying exception points to the main question whether the protection of databases is different from the balance of interests provided for in general copyright. Taking into account the special characteristic of investment protection inherent in the database right, this question has to be carefully considered.

A field of great concern also relates to the role of the database right in the research field. While the database right is still dormant in practice, its potential to have an impact on research activities is still underestimated. While the extension of the TDM exception to the database right goes a long way, making the research exception to the database right in Art. 9 Database Directive a mandatory exception could add to alleviating research activities in a digital environment that extends across borders and increase harmonisation of the legal framework. Within electronic research infrastructures, the search of whole databases should be permitted to reflect the realities of scientific work.[37]

It could be an option to introduce new specific limitations for the database right. This could apply to, e.g., search engines or web scraping where deficiencies in the interpretation of exisiting law are apparent. One problem with this approach is that the new limitations should be carefully tailored not to encroach on innovation and allow competitors to take unfair advantage of the efforts of the database maker. Moreover, introducing a new limitation each time new

---

[36] *Moreno* et al., Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, p. 77 et seqq.

[37] See the different usage scenarios in *Guibault/Wiebe* (eds.), Safe to be open: Study on the protection of research data and recommendations for access and usage, Göttingen, 2013, p. 118 et seqq.

technical features or service emerge would overstretch the law and be in possible conflict with the principle of technological neutrality.

IV. The *CV Melons* doctrine – flexible economic test as a solution?

A different solution seems to lie at hand when looking at the recent CJEU judgment in *CV Online v. Melons*. It shifts the scope of protection provided by the database right to a more flexible and economically imprinted approach reminiscent of unfair competition protection against misappropriation and slavish imitation. According to the Court, the Database Directive requires a fair balance to be struck between "on the one hand, the legitimate interest of the makers of databases in being able to redeem their substantial investment and, on the other hand, that of users and competitors of those makers in having access to the information contained in those databases and the possibility of creating innovative products based on that information"[38].

Adding a weighing of interest and a criterion of detriment to the investment to the infringement analysis resembling a fair use analysis in U.S. copyright law could obviate the introduction of new limitations. On the other hand, it may render questionable the legislative decision to exclude MGD from the database right in Art. 43 DA. Taking into account the relatively low investment costs for MGD, the test would mostly turn out on the no infringement side. Such an approach could achieve the same results without having to explicitly exclude MGD from the scope of the Data Act with the associated problems already discussed.

On the other hand, aggregated data sets and training data for AI might still be protected under the *CV Melons* test as well, which in turn might hinder data sharing.[39] But that is no different from the current situation where aggregated

---

[38] CJEU, Judgement of 3.6.2021, CV-Online Latvia, C-762/19, ECLI:EU:C:2021:434, para. 41. For an analysis *Derclaye/Husovec*, Sui Generis Database Protection 2.0: Judicial and Legislative Reforms, LSE Law, Society and Economy Working Papers 15 (5 et seqq.), 2022, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=4138436 (3.5.2024).

[39] See *Drexl* et al., 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), Max Planck Institute for Innovation and Competition Research Paper No 22-05, 2022, p. 92 n. 257; *Leistner/Antoine*, Study requested by the JURI Committee of the EP (n. 22), p. 53 et seq.

data do not fall into the scope of Art. 43 DA. To alleviate this problem a discussion may be revisited that was present in the drafting of the Database Directive but not implemented. A compulsory license as to sole source database was discussed but then discarded in favour of the differentiated scope of protection in Art. 7 Database Directive. Introducing such a scheme for this MGD including aggregated data may be a topic for future discussion.[40] With a projected increased emphasis on the enforcement of the database right the discussion of revising and amending the Databse Directive is far from over, espeiall with the rapid spread of AI applications and the connected enormous need for training data.

D. Resume and Conclusions

Art. 43 DA is not a perfect solution for the conflict between access rights in IoT-generated data and the database right. It carves out a specific exception that is vested with new problems of delineation in theory and practice. MGD have to be identified as coming from IoT devices or services. Aggregated data have to be discerned and excluded from the exception. New uncertainties arise as to whether dynamic mixed databases will be covered by the exception.

Currently, there does not seem to be a need for additional incentives to produce MGD as a ground for establishing new property rights.[41] But is it written in stone once and for all that no database rights are needed for creating a sufficient level of MGD databases in the future? If there is a policy decision to keep the database right in general there seems to be no reason to treat MGD differently. Overall, it would have been preferable to just rely on the CV Melons test and let the case law develop. While there might be fears that this would create considerable uncertainties as to access rights, case law could be working to clarify the issue. In addition, to avoid any uncertainties the legislator could have carved out the access rights under the Data Act as new limitations in Art. 9 Database Directive. Based on the existing law this could hint to interpreting Art. 43

---

[40] *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by European Parliament's Committee on Legal Affairs (JURI), Brussels, 2022, p. 62, 121.

[41] See *Kerber*, Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, GRUR Int. 2023, 120 (129).

DA this way as an elegant solution. However, as pointed out this might stretch the limits of interpretation too far.

digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Andreas Sattler & Herbert Zech (eds.)

The Data Act: First Assessments

In June 2023 the Weizenbaum Institute for the Networked Society, the Humboldt University of Berlin and the Center for Intellectual Property, Information and Technology Law (CIPLITEC) held a workshop on the – then just politically agreed – Data Act (DA). This volume contains the contributions based on the presentations by international experts, who participated in this workshop.

The EU Data Act: First Assessments sheds light on the interfaces between the DA and important other fields of law that the DA will have a great impact on. The First Assessments in this volume show that there are still various open questions and conflicts with different legal areas, posing fundamental challenges to achieving the objectives envisioned by the European legislator. This volume demonstrates that it will largely be up to the CJEU to successfully synchronise these legal interfaces, on which the DA so heavily depends.

Contributions written by:

- Martina Eckardt (Budapest, Hungary) & Wolfgang Kerber (Marburg, Germany)
- Bertin Martens (Brussels, Belgium)
- Thomas Weck (Frankfurt, Germany)
- Herbert Zech (Berlin, Germany)
- Axel Metzger (Berlin, Germany)
- Tanya Aplin (London, United Kingdom)
- Andreas Sattler (Karlsruhe, Germany)
- Benjamin Raue (Trier, Germany)
- Andreas Wiebe (Göttingen, Germany)